

2002 CERT Advisories

CERT Division

[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.

<http://www.sei.cmu.edu>



Copyright 2017 Carnegie Mellon University. All Rights Reserved.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

This report was prepared for the

SEI Administrative Agent
AFLCMC/AZS
5 Eglin Street
Hanscom AFB, MA 01731-2100

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

CERT® and CERT Coordination Center® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM17-0052

Table of Contents

1	CA-2002-01: Exploitation of Vulnerability in CDE Subprocess Control Service	1
2	CA-2002-02: Buffer Overflow in AOL ICQ	4
3	CA-2002-03: Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol (SNMP)	7
4	CA-2002-04: Buffer Overflow in Microsoft Internet Explorer	114
5	CA-2002-05: Multiple Vulnerabilities in PHP fileupload	118
6	CA-2002-06: Vulnerabilities in Various Implementations of the RADIUS Protocol	121
7	CA-2002-07: Double Free Bug in zlib Compression Library	130
8	CA-2002-08: Multiple Vulnerabilities in Oracle Servers	140
9	CA-2002-09: Multiple Vulnerabilities in Microsoft IIS	147
10	CA-2002-10: Format String Vulnerability in rpc.rwalld	151
11	CA-2002-11: Heap Overflow in Cachefs Daemon (cachefs)	154
12	CA-2002-12: Format String Vulnerability in ISC DHCPD	158
13	CA-2002-13: Buffer Overflow in Microsoft's MSN Chat ActiveX Control	163
14	CA-2002-14: Buffer overflow in Macromedia JRun	166
15	CA-2002-15: Denial-of-Service Vulnerability in ISC BIND 9	168
16	CA-2002-16: Multiple Vulnerabilities in Yahoo! Messenger	174
17	CA-2002-17: Apache Web Server Chunk Handling Vulnerability	178
18	CA-2002-18: OpenSSH Vulnerabilities in Challenge Response Handling	187
19	CA-2002-19: Buffer Overflows in Multiple DNS Resolver Libraries	198
20	CA-2002-20: Multiple Vulnerabilities in CDE ToolTalk	210
21	CA-2002-21: Vulnerability in PHP	217
22	CA-2002-22: Multiple Vulnerabilities in Microsoft SQL Server	222
23	CA-2002-23: Multiple Vulnerabilities In OpenSSL	229
24	CA-2002-24: Trojan Horse OpenSSH Distribution	236
25	CA-2002-25: Integer Overflow In XDR Library	240
26	CA-2002-26: Buffer Overflow in CDE ToolTalk	247
27	CA-2002-27: Apache/mod_ssl Worm	254
28	CA-2002-28: Trojan Horse Sendmail Distribution	261
29	CA-2002-29: Buffer Overflow in Kerberos Administration Daemon	265

30	CA-2002-30: Trojan Horse tcpdump and libpcap Distributions	272
31	CA-2002-31: Multiple Vulnerabilities in BIND	275
32	CA-2002-32: Backdoor in Alcatel OmniSwitch AOS	289
33	CA-2002-33: Heap Overflow Vulnerability in Microsoft Data Access Components (MDAC)	291
34	CA-2002-34: Buffer Overflow in Solaris X Window Font Service	294
35	CA-2002-35: Vulnerability in RaQ Server Appliances	299
36	CA-2002-36: CERT® Advisory CA-2002-36 Multiple Vulnerabilities in SSH Implementations	302
37	CA-2002-37: CERT® Advisory CA-2002-37 Buffer Overflow in Microsoft Windows Shell	310

1 CA-2002-01: Exploitation of Vulnerability in CDE Subprocess Control Service

Original release date: January 14, 2002

Last revised: --

Source: CERT/CC

A complete revision history can be found at the end of this file.

Systems Affected

- Systems running CDE

Overview

The CERT/CC has received credible reports of scanning and exploitation of Solaris systems running the CDE Subprocess Control Service buffer overflow vulnerability identified in [CA-2001-31](#) and discussed in [VU#172583](#).

I. Description

Since [CA-2001-31](#) was originally released last November, the CERT/CC has received reports of scanning for `dtspcd` (6112/tcp). Just recently, however, we have received credible reports of an exploit for Solaris systems. Using network traces provided by [The HoneyNet Project](#), we have confirmed that the `dtspcd` vulnerability identified in [CA-2001-31](#) and discussed in [VU#172583](#) is actively being exploited.

The Common Desktop Environment (CDE) is an integrated graphical user interface that runs on UNIX and Linux operating systems. The CDE Subprocess Control Service (`dtspcd`) is a network daemon that accepts requests from clients to execute commands and launch applications remotely. On systems running CDE, `dtspcd` is spawned by the Internet services daemon (typically `inetd` or `xinetd`) in response to a CDE client request. `dtspcd` is typically configured to run on port 6112/tcp with root privileges.

There is a remotely exploitable buffer overflow vulnerability in a shared library that is used by `dtspcd`. During client negotiation, `dtspcd` accepts a length value and subsequent data from the client without performing adequate input validation. As a result, a malicious client can manipulate data sent to `dtspcd` and cause a buffer overflow, potentially executing code with root privileges. The overflow occurs in a fixed-size 4K buffer that is exploited by the contents of one of the attack packets. The signature can be found at bytes 0x3e-0x41 in the following attack packet from a tcpdump log (lines may wrap):

```
09:46:04.378306 10.10.10.1.3592 > 10.10.10.2.6112: P 1:1449(1448)
ack 1 win 16060 <nop,nop,timestamp 463986683 4158792> (DF)
```

```

0x0000 4500 05dc a1ac 4000 3006 241c 0a0a 0a01 E.....@.0.$.....
0x0010 0a0a 0a02 0e08 17e0 fee2 c115 5f66 192f ...f....._f./
0x0020 8018 3ebc e1e9 0000 0101 080a 1ba7 dffb ..>.....
0x0030 003f 7548 3030 3030 3030 3032 3034 3130 .?uH000000020410
0x0040 3365 3030 3031 2020 3420 0000 0031 3000 3e0001..4....10.
0x0050 801c 4011 801c 4011 1080 0101 801c 4011 ..@...@.....@.
0x0060 801c 4011 801c 4011 801c 4011 801c 4011 ..@...@...@...@.
...

```

The value 0x103e in the ASCII (right) column above is interpreted by the server as the number of bytes in the packet to copy into the internal 4K (0x1000) buffer. Since 0x103e is greater than 0x1000, the last 0x3e bytes of the packet will overwrite memory after the end of the 4K buffer. This is the same compromise vector identified in [VU#172583](#).

It is important to note that several Internet-enabled games may also use port 6112/tcp as a legitimate part of their normal operation, therefore, not all network activity involving this service may be malicious. Network administrators monitoring this type of activity may wish to verify whether probes of this type are actually attempts to exploit [VU#172583](#).

Many common UNIX systems ship with CDE installed and enabled by default. To determine if your system is configured to run dtspcd, check for the following entries (lines may wrap):

```

in /etc/services

dtspc 6112/tcp

in /etc/inetd.conf

dtspc stream tcp nowait root /usr/dt/bin/dtspcd
/usr/dt/bin/dtspcd

```

Any system that does not run the CDE Subprocess Control Service is not vulnerable to this problem.

II. Impact

An attacker can execute arbitrary code with root privileges.

III. Solution

Apply a patch

[VU#172583](#) contains information from vendors who have provided information for this advisory. We will update the vulnerability note as we receive more information. If a vendor's name does not appear, then the CERT/CC did not hear from that vendor. Please contact your vendor directly.

Vendor information can be found in the "Systems Affected" section of VU#172583

<http://www.kb.cert.org/vuls/id/172583#systems>

Limit access to vulnerable service

Until patches are available and can be applied, you may wish to limit or block access to the Subprocess Control Service from untrusted networks such as the Internet. Using a firewall or other packet-filtering technology, block or restrict access to the port used by the Subprocess Control Service. As noted above, `dtspcd` is typically configured to listen on port 6112/tcp. It may be possible to use [TCP Wrapper](#) or a similar technology to provide improved access control and logging functionality for `dtspcd` connections. Keep in mind that blocking ports at a network perimeter does not protect the vulnerable service from the internal network. It is important to understand your network configuration and service requirements before deciding what changes are appropriate.

[TCP Wrapper](#) is available from

<ftp://ftp.porcupine.org/pub/security/index.html>

Disable vulnerable service

You may wish to consider disabling `dtspcd` by commenting out the appropriate entry in `/etc/inetd.conf`. As a best practice, the CERT/CC recommends disabling any services that are not explicitly required. As noted above, it is important to consider the consequences of such a change in your environment.

Appendix A References

1. <http://www.kb.cert.org/vuls/id/172583>
2. <http://www.cert.org/advisories/CA-2001-31.html>
3. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2001-0803>
4. <http://xforce.iss.net/alerts/advice101.php>
5. <http://www.opengroup.org/cde/>
6. <http://www.opengroup.org/desktop/faq/>

The CERT Coordination Center thanks [The Honeynet Project](#) for their assistance in providing network traces of the exploitation.

Authors: [Allen Householder](#) and [Art Manion](#)

Copyright 2002 Carnegie Mellon University

Revision History

January 14, 2002: Initial release

2 CA-2002-02: Buffer Overflow in AOL ICQ

Original release date: January 24, 2002

Last revised: --

Source: CERT/CC

A complete revision history can be found at the end of this file.

Systems Affected

- AOL Mirabilis ICQ Versions 2001A and prior
- Voice Video & Games plugin installed with AOL Mirabilis ICQ prior to version 2001B Beta v5.18 Build #3659

Overview

There is a remotely exploitable buffer overflow in ICQ. Attackers that are able to exploit the vulnerability may be able to execute arbitrary code with the privileges of the victim user. Full details are discussed in [VU#570167](#). An exploit is known to exist, but we do not believe it has been distributed in the wild. We have not seen active scanning for this vulnerability, nor have we received any reports of this vulnerability being exploited.

I. Description

ICQ is a program for communicating with other users over the Internet. ICQ is widely used (by over 122 million people according to [ICQ Inc](#), an [AOL Time Warner](#) owned subsidiary). A buffer overflow exists in the ICQ client for Windows. The buffer overflow occurs during the processing of a Voice Video & Games feature request message. This message is supposed to be a request from another ICQ user inviting the victim to participate interactively with a third-party application. In versions prior to 2001B, the buffer overflow occurs in code within the ICQ client. In version 2001B the code containing the buffer overflow was moved to an external plug-in.

Therefore, all versions prior to the latest build of 2001B are vulnerable. Upon connection to an AOL ICQ server, vulnerable builds of the 2001B client will be instructed by the server to disable the vulnerable plug-in. Since versions of the ICQ client prior to 2001B do not have an external plug-in to disable, they are vulnerable even after connecting to the server. AOL Time Warner is recommending all users of vulnerable versions of ICQ upgrade to [2001B Beta v5.18 Build #3659](#).

During normal operation, ICQ clients can exchange messages with one another through the ICQ servers or via a direct connection. The buffer overflow specifically occurs during the processing of the Voice Video & Games request via a Type, Length, Value (TLV) tuple with type 0x2711 from the ICQ server, or via a crafted direct connection request.

Some versions of the ICQ client open port 4000/UDP for client-server communication. Other versions open port 5190/TCP for this communication. As with the previously reported AIM vulnerability, AOL has modified the ICQ server infrastructure to filter malicious messages that attempt to exploit this vulnerability, preventing it from being exploited through an AOL ICQ server. Exploiting the vulnerability through other means (man-in-the-middle attacks, third-party ICQ servers, DNS spoofing, network sniffing, etc.) may still be possible. Also, since UDP packets can be broadcast on a network, a malicious TLV packet with a spoofed source IP address may be accepted as a legitimate server message.

The ICQ client also listens on a variably assigned TCP port for direct connection requests. A person who wishes to establish a direct connection can query an ICQ server for the IP address and listening port of the victim. Versions 2000A and prior accept direct connections from anyone by default. Later versions of ICQ can be configured to accept direct connections from anyone. **Since ICQ requests can be sent directly from one client to another, blocking requests through a central server is not a completely effective solution.** The effective solution is to apply a patch, when available, that fixes the buffer overflow, or upgrade to 2001B Beta v5.18 Build #3659 with the Voice Video & Games feature disabled.

This vulnerability has been assigned the identifier CAN-2002-0028 by the Common Vulnerabilities and Exposures (CVE) group:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0028>

II. Impact

A remote attacker can execute arbitrary code with the privileges of the victim user.

III. Solution

All users should upgrade to version 2001B Beta v5.18 Build #3659. There is currently no patch available for the ICQ plug-in for 2001B or versions of the ICQ client prior to 2001B. Version 2001B Beta v5.18 Build #3659's installer will delete the vulnerable plug-in. In addition, for users who log in to the server with versions of 2001B prior to Beta v5.18 Build #3659, access to the vulnerable plug-in will be disabled. Users with versions prior to 2001B must upgrade to mitigate this vulnerability.

Block ICQ/SMS requests at the firewall

Blocking connections to login.icq.com and access to ports 4000/UDP, 5190/TCP and the TCP port that your client chooses to listen on may prevent exploitation of this vulnerability. Note that the client may establish a new listening port each time it is run. Note also that this does not protect you from attacks within the perimeter of your firewall.

Block untrusted messages

ICQ permits the user to deny direct connections from anyone without authorization or accept direct connections from known peers only. We recommend denying direct connections from anyone

without authorization. By accepting direct connections from known peers, you may still be vulnerable to attacks that originate from known peers if the peer has been compromised.

Appendix A Vendor Information

This appendix contains information provided by vendors for this advisory. When vendors report new information to the CERT/CC, we update this section and note the changes in our revision history. If a particular vendor is not listed below, we have not received their comments.

AOL Time Warner

See <http://web.icq.com/help/quickhelp/1,,117,00.html>.

The CERT Coordination Center thanks Daniel Tan and AOL Time Warner for their assistance in discovering and analyzing this vulnerability.

Author: Jason A. Rafail

Appendix B References

1. <http://www.kb.cert.org/vuls/id/570167>
2. <http://www.securityfocus.com/bid/3813>
3. <http://web.icq.com/help/quickhelp/1,,117,00.html>

Copyright 2002 Carnegie Mellon University

Revision History

January 24, 2002: Initial release

3 CA-2002-03: Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol (SNMP)

Original release date: February 12, 2002

Last revised: February 13, 2008

Source: CERT/CC

A complete revision history can be found at the end of this file.

Systems Affected

Products from a very wide variety of vendors may be affected. See Vendor Information for details from vendors who have provided feedback for this advisory.

In addition to the vendors who provided feedback for this advisory, a list of vendors whom CERT/CC contacted regarding these problems is available from

<http://www.kb.cert.org/vuls/id/854306>

<http://www.kb.cert.org/vuls/id/107186>

Many other systems making use of SNMP may also be vulnerable but were not specifically tested.

Overview

Numerous vulnerabilities have been reported in multiple vendors' SNMP implementations. These vulnerabilities may allow unauthorized privileged access, denial-of-service attacks, or cause unstable behavior. If your site uses SNMP in any capacity, the CERT/CC encourages you to read this advisory and follow the advice provided in the Solution section below.

In addition to this advisory, we also have a FAQ available at

http://www.cert.org/tech_tips/snmp_faq.html.

I. Description

The Simple Network Management Protocol (SNMP) is a widely deployed protocol that is commonly used to monitor and manage network devices. Version 1 of the protocol (SNMPv1) defines several types of SNMP messages that are used to request information or configuration changes, respond to requests, enumerate SNMP objects, and send unsolicited alerts. The Oulu University Secure Programming Group (OUSPG, <http://www.ee.oulu.fi/research/ouspg/>) has reported numerous vulnerabilities in SNMPv1 implementations from many different vendors. More information about SNMP and OUSPG can be found in Appendix C.

OUSPG's research focused on the manner in which SNMPv1 agents and managers handle request and trap messages. By applying the PROTOS c06-snmpv1 test suite (<http://www.ee.oulu.fi/research/ouspg/protos/testing/c06/snmpv1/0100.html>) to a variety of popular SNMPv1-enabled products, the OUSPG revealed the following vulnerabilities:

VU#107186 - Multiple vulnerabilities in SNMPv1 trap handling

SNMP trap messages are sent from agents to managers. A trap message may indicate a warning or error condition or otherwise notify the manager about the agent's state. SNMP managers must properly decode trap messages and process the resulting data. In testing, OUSPG found multiple vulnerabilities in the way many SNMP managers decode and process SNMP trap messages.

VU#854306 - Multiple vulnerabilities in SNMPv1 request handling

SNMP request messages are sent from managers to agents. Request messages might be issued to obtain information from an agent or to instruct the agent to configure the host device. SNMP agents must properly decode request messages and process the resulting data. In testing, OUSPG found multiple vulnerabilities in the way many SNMP agents decode and process SNMP request messages.

Vulnerabilities in the decoding and subsequent processing of SNMP messages by both managers and agents may result in denial-of-service conditions, format string vulnerabilities, and buffer overflows. Some vulnerabilities do not require the SNMP message to use the correct SNMP community string.

These vulnerabilities have been assigned the CVE identifiers CAN-2002-0012 and CAN-2002-0013, respectively.

II. Impact

These vulnerabilities may cause denial-of-service conditions, service interruptions, and in some cases may allow an attacker to gain access to the affected device. Specific impacts will vary from product to product.

III. Solution

Note that many of the mitigation steps recommended below may have significant impact on your everyday network operations and/or network architecture. Ensure that any changes made based on the following recommendations will not unacceptably affect your ongoing network operations capability.

Apply a patch from your vendor

Appendix A contains information provided by vendors for this advisory. Please consult this appendix to determine if you need to contact your vendor directly.

Disable the SNMP service

As a general rule, the CERT/CC recommends disabling any service or capability that is not explicitly required, including SNMP. Unfortunately, some of the affected products exhibited unexpected behavior or denial of service conditions when exposed to the OUSPG test suite *even if SNMP was not enabled*. In these cases, disabling SNMP should be used in conjunction with the filtering practices listed below to provide additional protection.

Ingress filtering

As a temporary measure, it may be possible to limit the scope of these vulnerabilities by blocking access to SNMP services at the network perimeter.

Ingress filtering manages the flow of traffic as it enters a network under your administrative control. Servers are typically the only machines that need to accept inbound traffic from the public Internet. In the network usage policy of many sites, there are few reasons for external hosts to initiate inbound traffic to machines that provide no public services. Thus, ingress filtering should be performed at the border to prohibit externally initiated inbound traffic to non-authorized services. For SNMP, ingress filtering of the following ports can prevent attackers outside of your network from impacting vulnerable devices in the local network that are not explicitly authorized to provide public SNMP services.

```
snmp 161/udp # Simple Network Management Protocol (SNMP)
snmp 162/udp # SNMP system management messages
```

The following services are less common, but may be used on some affected products

```
snmp 161/tcp # Simple Network Management Protocol (SNMP)
snmp 162/tcp # SNMP system management messages
smux 199/tcp # SNMP Unix Multiplexer
smux 199/udp # SNMP Unix Multiplexer
synoptics-relay 391/tcp # SynOptics SNMP Relay Port
synoptics-relay 391/udp # SynOptics SNMP Relay Port
agentx 705/tcp # AgentX
snmp-tcp-port 1993/tcp # cisco SNMP TCP port
snmp-tcp-port 1993/udp # cisco SNMP TCP port
```

As noted above, you should carefully consider the impact of blocking services that you may be using.

It is important to note that in many SNMP implementations, the SNMP daemon may bind to all IP interfaces on the device. This has important consequences when considering appropriate packet filtering measures required to protect an SNMP-enabled device. For example, even if a device disallows SNMP packets directed to the IP addresses of its normal network interfaces, it may still be possible to exploit these vulnerabilities on that device through the use of packets directed at the following IP addresses:

- "all-ones" broadcast address
- subnet broadcast address
- any internal loopback addresses (commonly used in routers for management purposes, not to be confused with the IP stack loopback address 127.0.0.1)

Careful consideration should be given to addresses of the types mentioned above by sites planning for packet filtering as part of their mitigation strategy for these vulnerabilities.

Finally, sites may wish to block access to the following RPC services related to SNMP (listed as name, program ID, alternate names)

```
snmp 100122 na.snmp snmp-cmc snmp-synoptics snmp-unisys snmp-utk
snmpv2 100138 na.snmpv2 # SNM Version 2.2.2
snmpXdmid 100249
```

Please note that this workaround may not protect vulnerable devices from internal attacks.

Filter SNMP traffic from non-authorized internal hosts

In many networks, only a limited number of network management systems need to originate SNMP request messages. Therefore, it may be possible to configure the SNMP agent systems (or the network devices in between the management and agent systems) to disallow request messages from non-authorized systems. This can reduce, but not wholly eliminate, the risk from internal attacks. However, it may have detrimental effects on network performance due to the increased load imposed by the filtering, so careful consideration is required before implementation. Similar caveats to the previous workaround regarding broadcast and loopback addresses apply.

Change default community strings

Most SNMP-enabled products ship with default community strings of "public" for read-only access and "private" for read-write access. As with any known default access control mechanism, the CERT/CC recommends that network administrators change these community strings to something of their own choosing. However, even when community strings are changed from their defaults, they will still be passed in plaintext and are therefore subject to packet sniffing attacks. SNMPv3 offers additional capabilities to ensure authentication and privacy as described in RFC2574.

Because many of the vulnerabilities identified in this advisory occur before the community strings are evaluated, it is important to note that performing this step alone is **not** sufficient to mitigate the impact of these vulnerabilities. Nonetheless, it should be performed as part of good security practice.

Segregate SNMP traffic onto a separate management network

In situations where blocking or disabling SNMP is not possible, exposure to these vulnerabilities may be limited by restricting all SNMP access to separate, isolated management networks that are not publicly accessible. Although this would ideally involve physically separate networks, that kind of separation is probably not feasible in most environments. Mechanisms such as virtual

LANs (VLANs) may be used to help segregate traffic on the same physical network. Note that VLANs may not strictly prevent an attacker from exploiting these vulnerabilities, but they may make it more difficult to initiate the attacks.

Another option is for sites to restrict SNMP traffic to separate virtual private networks (VPNs), which employ cryptographically strong authentication.

Note that these solutions may require extensive changes to a site's network architecture.

Egress filtering

Egress filtering manages the flow of traffic as it leaves a network under your administrative control. There is typically limited need for machines providing public services to initiate outbound traffic to the Internet. In the case of SNMP vulnerabilities, employing egress filtering on the ports listed above at your network border can prevent your network from being used as a source for attacks on other sites.

Share tools and techniques

Because dealing with these vulnerabilities to systems and networks is so complex, the CERT/CC will provide a forum where administrators can share ideas and techniques that can be used to develop proper defenses. We have created an unmoderated mailing list for system and network administrators to discuss helpful techniques and tools.

You can subscribe to the mailing list by sending an email message to majordomo@cert.org. In the body of the message, type

subscribe snmp-forum

After you receive the confirmation message, follow the instructions in the message to complete the subscription process.

Appendix A Vendor Information

This appendix contains information provided by vendors for this advisory. As vendors report new information to the CERT/CC, we will update this section and note the changes in our revision history. If a particular vendor is not listed below, we have not received their comments.

ADTRAN, Inc.

ADTRAN Advisory:
SNMPv1 Request and Trap Handling Vulnerabilities
Revision 1.0
Release Date: 19 February 2002

I. Summary

On February 12, 2002 the CERT®/CC released an advisory related to security vulnerabilities that

may exist in network devices using SNMPv1 as the management protocol. In response to this advisory, CERT® Advisory CA-2002-03 Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol (SNMP)", ADTRAN began executing the tests that elicit these vulnerabilities for all ADTRAN products that feature SNMPv1 capability.

II. Impact

Preliminary test results have indicated multiple ADTRAN products exhibit certain vulnerabilities to SNMP messages. Some of these vulnerabilities can be exploited, resulting in a denial of service or service interruption. These results have not indicated any vulnerability that will allow an attacker to gain access to the affected device.

III. Solution

ADTRAN is currently applying the PROTOS c06-SNMPv1 test suite to all products that feature SNMPv1 capability. Until ADTRAN has completed testing on all of its products and provided patches or fixes to eliminate these vulnerabilities, ADTRAN recommends considering one or more of the following solutions, as identified in CERT® Advisory CA-2002-03, to minimize your network's potential exposure to these vulnerabilities:

- Disable the SNMP Service
- Ingress filtering
- Egress filtering
- Filter SNMP traffic from non-authorized internal hosts
- Segregate SNMP traffic onto a separate management network
- Restrict SNMP traffic to Virtual Private Networks (VPNs)
- Change default community strings

ADTRAN's NetVanta Solutions

ADTRAN's NetVanta 2000 Series of products can be used to provide most of the solutions identified above, including ingress and egress filtering, filtering SNMP traffic from non-authorized internal hosts, and restricting SNMP traffic to Virtual Private Networks (VPNs). For further information on how NetVanta's VPN and Firewall solutions can secure your network, please see <http://www.adtran.com/netvanta2000>.

IV. For Further Information

For more information please see <http://www.adtran.com/support/snmp>.

AdventNet

This is in reference to your notification regarding [VU#107186 and VU#854306] and OUSPG#0100. AdventNet Inc. has reproduced this behavior in their products and coded a Service Pack fix which is currently in regression testing in AdventNet Inc.'s Q.A. organization. The release of AdventNet Inc.'s Service Pack correcting the behavior outlined in [... OUSPG#0100] is scheduled to be generally available to all of AdventNet Inc.'s customers by February 20, 2002.

ADVA AG Optical Networking

ADVA Optical Networking is addressing the SNMP vulnerabilities identified in the advisory CA-2002-03 across the entire product line.

ADVA is currently applying the test suite provided by OUSPG (PROTOS c06-snmpv1 test suite) to all of its products.

Following products are tested against possible effects of the vulnerability report VU#854306 - Multiple vulnerabilities in SNMPv1 request:

FSP 3000
FSP 2000
FSP II
FSP I
FSP 1000
FSP 500
CELL-ACE
CELL-ACE-PLUS

The ADVA Network Management products:

FSP Element Manager
FSP Network Manager
CELL-SCOPE

are tested against vulnerabilities of the report VU#107186 - Multiple vulnerabilities in SNMPv1 trap handling.

The ongoing tests have not unveiled vulnerabilities so far.

Test results and information about product updates will be published on the ADVA Optical Networking web site: <http://www.advaoptical.com>.

Alcatel

The security of our customers' networks is of highest priority for Alcatel. Alcatel is aware of this industry-wide SNMP security issue and has put measures in place to assess which of its products might be affected. Within this activity, Alcatel is closely working with its customers and CERT to address and fix potential security problems as identified by CERT.

Allied Telesyn International

Please see <http://www.kb.cert.org/vuls/id/IAFY-56DKQY>.

Alvarion Ltd.

In response to CERT® Advisory CA-2002-03 regarding multiple vulnerabilities in many implementations of the Simple Network Management Protocol (SNMP), Alvarion performed a varied and thorough set of tests on its BreezeACCESS and WALKair products. The tests performed are the ones recommended by the PROTOS project paper.

Following these tests, Alvarion found no denial of service, memory corruption, stack corruption or other fatal error conditions in its BreezeACCESS and WALKair products.

In addition, Alvarion's BreezeACCESS and WALKair products implement the following additional security measures which are recommended by the PROTOS project report:

1. Perimeter filtering to SNMP traffic.
2. SNMP device based network access control to filter the traffic.
3. Isolation of SNMP traffic into a separate management VLAN (applicable for BreezeACCESS II, XL and MMDS).

American Power Conversion

American Power Conversion has conducted extensive testing in order to determine the impact any vulnerabilities within SNMP pose to our customers. We have determined that exploiting these vulnerabilities in some versions of our firmware can interfere with the normal operation of APC's SNMP-enabled products.

Upgrades are available that repair these vulnerabilities.

For details, refer to the APC Knowledge Base document titled " American Power Conversion Security Bulletin" available at www.apc.com.

Apple Computer, Inc.

The only product currently shipping with SNMP software is the AirPort Base Station. The AirPort Base Station has been tested and no security vulnerabilities associated with advisory CA-2002-03 have been found.

Aprisma

As mentioned within Aprisma's February 2002 CERT advisory statement, we have performed the necessary SPECTRUM (6.0 rev3 and 6.5) tests required to address CERT Advisory CA-2002-03, VU#107186 - PROTOS Test-Suite: c06-SNMPv1.

Aprisma's comprehensive testing has revealed less than ten SNMP message tests - out of thousands of individual tests conducted - exhibited irregular system behavior. As a result of these findings, Aprisma is issuing the following patches to protect our customers against known SNMPv1 vulnerabilities:

CERT Advisory CA-2002-03

VU#107186 - Multiple Vulnerabilities in SNMPv1 Trap Handling:

- Patch 71 for SPECTRUM 6.0 rev3
- Patch 22 for SPECTRUM 6.5 (SPECTRUM infinitya, SPECTRUM integritya, and SPECTRUM xsighta)

For customer convenience, Aprisma has combined previously released patches (Patches 9 and 21 for SPECTRUM 6.5), that help prevent a SNMPv1 trap-related vulnerability, into the aforementioned Patch 22 for SPECTRUM 6.5.

It is recommended that all SPECTRUM customers, who have not taken alternative measures to secure their SPECTRUM servers from SNMPv1 vulnerabilities, install the appropriate patch immediately when available. Patches will be made available over the next several weeks.

Asante Technologies, Inc.

Asante manufactures and supplies a large range of SNMP managed enterprise LAN switches and related products. The following products have been fully tested and are found NOT to be affected by the SNMP vulnerabilities outlined in VU#854306 and VU#107186.

6524 - 24 port 10/100 switch with 2 GBIC's
3524 - 24 port 10/100 stackable switch with 2 GBE slots
8000 - 24 port 10/100 modular stackable switch with 3 GBE slots
6014 - 12 port 10/100 IntraStack Switch
2072 - Chassis based modular solution
Netstacker II - 24 port 10/100 stackable hub with MII slot
FriendlyNET range of products.

Asante is continuing to address possible vulnerabilities across its entire FriendlyNET, IntraCore and all other product lines. Please contact support@asante.com for further information.

Astracon, Inc.

The Astracon Stinger NetConnect is safe against the vulnerability reported by VU#107186. The Stinger NetConnect processes SNMP responses only. Since the trap demon is never invoked, the Stinger NetConnect will never receive a trap; it is always safe.

The Stinger NetConnect doesn't accept SNMP requests, but can send SNMP version 1 or version 3 requests. By configuring the NetConnect to use only SNMP version 3, the vulnerabilities caused when using SNMP version 1 in the network will be avoided.

In order to ensure safety against the vulnerability reported by VU#854306 and VU#107186, the test cases at <http://www.ee.oulu.fi/research/ouspg/protos/testing/c06/snmpv1/> were executed, with no adverse effect on the NetConnect. The Stinger NetConnect passed all of the test cases.

Avaya

Avaya is addressing the vulnerabilities identified in this advisory. The latest information on the affect of this vulnerability on Avaya products can be found at: <http://support.avaya.com/security>

AVET Information and Network Security

AVET FireBorder OS (any version, including 1.4) is not vulnerable to the following vulnerabilities: - CAN-2002-0012 - CAN-2002-0013

This is due to several reasons:

- AVET FireBorder OS does not contain SNMP server
- administrator user can not install SNMP server due to lack of privileges
- system architecture would not allow to run arbitrary code in any of running network daemons; theoretically under some circumstances it could be possible to perform remote DoS attack on vulnerable servers; still to install and run SNMP daemon local user would need to bypass default permission and ACL settings.

Avici Systems Inc.

Avici Systems has tested the TSR and SSR product lines, including all associated line card modules according to recommendations issued by CERT, and has found no security vulnerabilities associated with Advisory CA-2002-03 (Multiple Vulnerabilities in Many Implementations of SNMP).

BinTec Communications AG

BinTec Communications announces that SNMP vulnerability VU#854306 reported in March has been resolved with System Software Release 6.2.1. If you do not wish to use the workarounds suggested in March in order to obviate possible exploits of VU#854306, you can update your system. The software is currently available as BETA software from www.bintec.net, and the final release is expected in June.

Please, note that BETA software is susceptible to malfunctions, and that BinTec Communications does not assume responsibility for any problems arising from the use of BETA software. If you do not want to use System Software Release 6.2.1 BETA, you can still use the workarounds suggested in our initial statement.

BMC Software

BMC Software, Inc. has completed its analysis of this security advisory and has posted detailed information to its web site. Specific product information is referenced at the following location:
http://www.bmc.com/info_center_support/snmp_cert_advise041802.html.

BMC's Patrol Agent was found to require a patch to fix problems found when running the test suite from Oulu University Secure Programming Group. Information on this patch can be found by referencing the above page or reviewing Problem Resolution ID 116035 from the BMC Support website, <http://www.bmc.com/support.html>. The BMC DevCon SNMP forum at <http://devcon.bmc.com/> also has information about the PATROL patches.

Other information about this alert is also available on the BMC Support

website, under News at "SNMP Advisory Posted by CERT", the direct reference to this page is:

http://www.bmc.com/info_center_support/news_detail/0,2561,18962_0_125215,00.html .

CacheFlow

The purpose of this email is to advise you that CacheFlow Inc. has provided a software update. Please be advised that updated versions of the software are now available for all supported CacheFlow hardware platforms, and may be obtained by CacheFlow customers at the following URL:

<http://download.cacheflow.com/>

The specific reference to the software update is contained within the Release Notes for CacheOS Versions 3.1.22 Release ID 17146, 4.0.15 Release ID 17148, 4.1.02 Release ID 17144 and 4.0.15 Release ID 17149.

RELEASE NOTES FOR CACHEFLOW SERVER ACCELERATOR PRODUCTS:

- <http://download.cacheflow.com/release/SA/4.0.15/relnotes.htm>

RELEASE NOTES FOR CACHEFLOW CONTENT ACCELERATOR PRODUCTS:

- <http://download.cacheflow.com/release/CA/3.1.22/relnotes.htm>
- <http://download.cacheflow.com/release/CA/4.0.15/relnotes.htm>
- <http://download.cacheflow.com/release/CA/4.1.02/relnotes.htm>

* SR 1-1647517, VI 13045: This update modified a potential vulnerability by using an SNMP test tools exploit.

3Com Corporation

A vulnerability to an SNMP packet with an invalid length community string has been resolved in the following products. Customers concerned about this weakness should ensure that they upgrade to the following agent versions:

PS Hub 40

2.16 is due Feb 2002

PS Hub 50

2.16 is due Feb 2002

Dual Speed Hub

2.16 is due Jan 2002

Switch 1100/3300

2.68 is available now

Switch 4400

2.02 is available now

Switch 4900

2.04 is available now

WebCache1000/3000

2.00 is due Jan 2002

For updated information on CommWorks Corporation, a 3Com company, visit http://www.commworks.com/Press/Archive/2002/February/CERT_Advisory.asp

In addition, CommWorks' customers should monitor http://totalservice.commworks.com/cert_update.cfm for updated information addressing the CERT advisory, as well as information on available patches for CommWorks' products.

Caldera

Caldera International, Inc. has reproduced faulty behavior in Caldera SCO OpenServer 5, Caldera UnixWare 7, and Caldera Open UNIX 8. We have coded a software fix for supported versions of Caldera UnixWare 7 and Caldera Open UNIX 8 that will be available from our support site at <http://stage.caldera.com/support/security> immediately following the publication of this CERT announcement. A fix for supported versions of OpenServer 5 will be available at a later date.

Cambridge Broadband Ltd.

Cambridge Broadband's products use the ucd-snmp package, version 4.2.3, with proprietary extensions. We have tested our build of the software with the OUSPG test suites and determined that it is not susceptible to these vulnerabilities.

Canoga Perkins Corporation

Please see http://www.canoga.com/technical_bulletins.htm

Carrier Access

Carrier Access has reviewed the released CERT® Advisory CA-2002-03 related to security vulnerabilities that exist in network devices using SNMPv1 as the management protocol.

There are no known format string or buffer overflow vulnerabilities. Denial of service (management) is a known vulnerability of Carrier Access products residing on non-secure networks. Specific testing and a review of test reports have revealed no SNMP V1 security issues. Carrier Access has documented this finding in a Product Technical Note (PTN-02-003). To receive a copy of this documentation, please contact Carrier Access customer support center at 1-800-786-9929 or email to "tech-support@carrieraccess.com"

Recommended Actions for Network Security:

- . Review and implementation of accepted solutions outlined in section III (Solution) of CERT ®

Advisory CA-2002-03

- . Filter of SNMP traffic at network access points
- . Use of proprietary SNMP Community Strings
- . Segregate/Filter Network Management traffic from public domains

Check Point Software Technologies Inc.

Check Point Statement on SNMP Vulnerability Test Suite

Recently, an automated suite has been released which tests products for known SNMP vulnerabilities.

FireWall-1, by default, blocks all SNMP communication to, from, or across a FireWall-1 gateway. SNMP communication is enabled only if the administrator writes a specific rule which allows the communication.

SNMP communication is not required for correct functionality of any Check Point products.

If SNMP monitoring of Check Point firewalls is needed, Check Point recommends that the FireWall-1 rule base tightly restrict SNMP communication and that all relevant operating system security patches be applied.

Check Point knows of no SNMP-related security issues in any of its products, and has conducted an extensive review to ensure that none exist.

CipherTrust, Inc.

This is in reference to your notification regarding VU#107186 and VU#854306. CipherTrust has confirmed that IronMail is not vulnerable to these issues. IronMail allows alert notification via SNMP traps. This allows the IronMail to be integrated into SNMP managed services without being open to vulnerabilities such as these. Specifically, due to the way that IronMail uses SNMP, it does not receive requests or traps.

Cisco Systems

Cisco Systems is addressing the vulnerabilities identified by VU#854306 and VU#107186 across its entire product line. Cisco has released an advisory:

<http://www.cisco.com/warp/public/707/cisco-malformed-snmp-msgs-pub.shtml>

CNT

Overview

On February 12, 2002, the CERT® Coordination Center of Carnegie-Mellon University issued an advisory identifying possible security vulnerabilities of multiple vendor products that utilize the Simple Network Management Protocol (SNMP) for management of those products. This advisory was based on research done by the University of Oulu in Finland. The complete advisory may be

found on the CERT web site at: <http://www.cert.org/advisories/CA-2002-03.html>. If your site uses SNMP-based CNT products in any capacity, we encourage you to read this advisory.

I. Description

The Simple Network Management Protocol (SNMP) is a widely deployed protocol that is commonly used to monitor and manage network devices. Version 1 of the protocol (SNMPv1) defines several types of SNMP messages that are used to request information or configuration changes, respond to requests, enumerate SNMP objects, and send unsolicited alerts. The Oulu University Secure Programming Group (OUSPG, <http://www.ee.oulu.fi/research/ouspg/>) has reported vulnerabilities in SNMPv1 implementations from many different vendors. OUSPG's research focused on the manner in which SNMPv1 agents and managers handle request and trap messages. By applying the PROTOS c06-snmpv1 test suite (<http://www.ee.oulu.fi/research/ouspg/protos/testing/c06/snmpv1/0100.html>) to a variety of popular SNMPv1-enabled products, the OUSPG revealed the following vulnerabilities:

VU#107186 - Multiple vulnerabilities in SNMPv1 trap handling

SNMP trap messages are sent from agents to managers. A trap message may indicate a warning or error condition or otherwise notify the manager about the agent's state. SNMP managers must properly decode trap messages and process the resulting data. In testing, OUSPG found multiple vulnerabilities in the way many SNMP managers decode and process SNMP trap messages.

VU#854306 - Multiple vulnerabilities in SNMPv1 request handling

SNMP request messages are sent from managers to agents. Request messages might be issued to obtain information from an agent or to instruct the agent to configure the host device. SNMP agents must properly decode request messages and process the resulting data. In testing, OUSPG found multiple vulnerabilities in the way many SNMP agents decode and process SNMP request messages.

Vulnerabilities in the decoding and subsequent processing of SNMP messages by both managers and agents may result in denial-of-service conditions, format string vulnerabilities, and buffer overflows. Some vulnerabilities do not require the SNMP message to use the correct SNMP community string.

II. CNT® Products

CNT has a number of products affected by the SNMP vulnerabilities described above. Each CNT product with SNMP functionality is described below along with the specific vulnerability, or lack thereof, of that product and the recommended procedures to follow with that product.

- UltraNet® Storage Director
The UltraNet Storage Director (USD) was tested with the PROTOS test suite. Two tests caused snmpd on the USD to abort and restart; the snmpd responded to requests specifying a community string beginning with a null; several minor ASN.1 / BER handling discrepancies related to invalid encodings were noted. Corrective code for the snmpd aborts and the community string handling issue has been developed and successfully tested. This code will be made available in the USD 2.7

software release, currently scheduled for availability in April 2002. The ASN.1 / BER invalid encoding handling issues will be addressed in a future release. CNT recommends upgrading to the USD 2.7 software release as soon as it is available.

- **UltraNet Edge Storage Router**
The UltraNet Edge Storage Router (Edge) was tested with the PROTOS test suite. Three tests caused the Edge to hang or abort, requiring a reboot. Corrective code for these errors has been developed and successfully tested. The Edge responded to requests specifying a bad SNMP version number; several minor ASN.1 / BER handling discrepancies related to invalid encodings were noted. The responded to bad SNMP version number and the ASN.1 / BER invalid encoding handling issues will be addressed in a future release. This code will be made available in the Edge software release 1.4.1, currently scheduled for release in April 2002. CNT recommends upgrading the Edge to release 1.4.1 as soon as it is available.
- **Channelink®**
The Channelink product was tested with the PROTOS test suite. All tests ran successfully. No failures occurred. No corrective action is required with the Channelink product.
- **WebView**
The WebView SNMP-based element manager was tested with the PROTOS test suite. WebView is not affected by the recent SNMP vulnerabilities found by CERT. No corrective action is required with the WebView product.
- **UltraNet CMF**
The CastleRock software upon which CNT's UltraNet CMF SNMP-based management software is based was tested with the PROTOS test suite. CastleRock has reported two test failures. Corrective code for these errors has been developed and is now being tested within UltraNet CMF. This code will be made available in the CMF release 6.4, currently scheduled for release in early May 2002. CNT recommends upgrading CMF to release 6.4 as soon as it is available.

III. CNT Product Upgrades

CNT will continue to test new releases of its products against the PROTOS test suite to ensure that additional vulnerabilities are not introduced as a result of any new releases.

To determine whether a new CNT product release is available and how to upgrade to that release when available, contact CNT Technical Support (800-752-8061 or 763-268-6600) or contact your company's CNT Technical Account Engineer (TAE).

Compaq Computer Corporation

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

TITLE: (SSRT0779) Potential Security Vulnerabilities in SNMP
Posted at <http://ftp.support.compaq.com/patches/.new/security.shtml>

NOTICE: There are no restrictions for distribution of this
Bulletin provided that it remains complete and intact.

RELEASE DATE: 18 FEBRUARY, 2002

UPDATED: 03 APRIL, 2002 - update Tru64, patch availability
08 MARCH, 2002 - add StorageWorks products, and
Compaq/Microcom based products.
05 MARCH, 2002 - update TRU64 Information

SEVERITY: MEDIUM

SOURCE: Compaq Computer Corporation
Compaq Global Services
Software Security Response Team

CROSS REFERENCE: (SSRT0799, CAN-2002-0012,
CAN-2002-0013, CERT CA-2002-03)

PROBLEM SUMMARY:

The Computer Emergency Response Team (CERT/cc) has recently issued an advisory regarding numerous potential vulnerabilities in SNMPv1 implementations. These potential vulnerabilities are applicable to SNMPv1 trap handling and SNMPv1 Request handling. The CERT article outlines vulnerabilities that can cause SNMP services to stop functioning and in some cases may enable "unauthorized access," "denial of service attacks" or may cause system instability.

IMPACT:

Compaq NonStop Himalaya Servers:
Compaq TCP/IP Services for OpenVMS:
Compaq Tru64 UNIX:
Compaq Insight Management Suite:
Compaq Deskpro, Professional Workstation, Armada, Evo:
Compaq SANworks Hardware:
Compaq StorageWorks Products
Compaq/Microcom Products:

Compaq's findings to date regarding the SNMPv1 issues are as follows:

Compaq NonStop Himalaya Servers:

The Compaq Himalaya NonStop Kernel prohibits execution of code on the stack or heap by hardware TLB permissions (read/write only), preventing Trojan horse attacks by embedding code within the buffer overflow area. However, process ABENDs can occur.

The SNMP agent ABENDs in the c06-snmv1 buffer-overflow tests. This affects forwarding trap messages and/or sending info responses to SNMP managers.

Sub-agents use IPCs to communicate with the SNMP agent, so they cannot be directly attacked. More importantly, sub-agents are confined to information only requests, so they cannot be used to configure/manage their sub-systems. Our investigation and analysis is continuing and further updates will be provided.

IPMs to address the ABEND problem of the SNMP are in development and will be released as soon as verification is complete. Availability of these IPMs will be announced in future updates. The exposure to SNMP agent ABENDs can be reduced by running the SNMP agent as a process-pair or by configuring auto-restart in the Persistence Manager.

Compaq TCP/IP Services for OpenVMS:

There is some impact to the SNMP agent provided with Compaq TCP/IP Services for OpenVMS. This problem can cause the SNMP agent to ACCVIO and terminate temporarily denying service to SNMP, but in most cases after this occurs Compaq TCP/IP Services for OpenVMS will restart the SNMP agent in response to the next SNMP request. There are no known risks of compromising system security due to this problem. The SNMP agent executes from a non-privileged process, which prevents any compromise to system security.

Our investigation and analysis has determined the cause of the problem. The updated images for Compaq TCP/IP Services for OpenVMS are now in final test. Compaq will provide updates to Compaq TCP/IP Services for OpenVMS in the next ECO and also in the next release, Compaq TCP/IP Services for OpenVMS V5.3. Contact Compaq's Customer Support Center if an earlier updated is required.

Compaq Tru64 UNIX:

UPDATE: 02 April, 2002

There is no known risk of compromising Tru64 UNIX system security due to the recent SNMP attack. The SNMP agent provided with

Tru64 UNIX is susceptible to a limited problem - the SNMP agent may stop responding to SNMP requests, or it may incur a segmentation fault, generate a core file, and exit. Either scenario denies SNMP service to SNMP-based network management applications. However, we have not found the attack to cause the system to be unstable, vulnerable to "unauthorized access", or subject to any denial of service other than to the SNMP service.

Impacted Tru64 UNIX operating system versions include:
Tru64 UNIX 4.0f, 4.0g, 5.0a, 5.1, 5.1a.

SOLUTION:

Until the Tru64 UNIX fixes are available in the mainstream release patch kits, Compaq is releasing the following Early Release Patch Kit(s) (ERPs) publicly for use by any customer.

The Early Release Patch kits use dupatch to install and will not install over any Customer-Specific-Patches (CSPs) which have file intersections with the ERPs. Raise an IPMT case to UNIX Support Engineering if you need a CSP merged with one of the following ERPs.

The fixes contained in the Early Release Patch (ERP) kits will be available in the next mainstream patch kit(s) for:

- Tru64 UNIX 4.0F PK8
- Tru64 UNIX 4.0G PK4
- Tru64 UNIX 5.0A PK4
- Tru64 UNIX 5.1 PK5
- Tru64 UNIX 5.1A PK2

Early Release Patches

Tru64 UNIX 4.0F

PREREQUISITE: Tru64 UNIX 4.0F with PK7 (BL18) installed
ERP Kit Name: DUV40FB18-C0071301-13866-ES-20020401
Kit Location: <http://ftp1.support.compaq.com/public/unix/v4.0f/>

Tru64 UNIX 4.0G

PREREQUISITE: Tru64 UNIX 4.0G with PK3 (BL17) installed
ERP Kit Name: T64V40GB17-C0012100-13640-ES-20020313

Kit Location: <http://ftp1.support.compaq.com/public/unix/v4.0g/>

Tru64 UNIX 5.0A

PREREQUISITE: Tru64 UNIX 5.0A with PK3 (BL17) installed

ERP Kit Name: T64V50AB17-C0019600-13593-ES-20020308

Kit Location: <http://ftp1.support.compaq.com/public/unix/v5.0a/>

Tru64 UNIX 5.1

PREREQUISITE: Tru64 UNIX 5.1 with PK4 (BL18) installed

ERP Kit Name: T64V51B18-C0109002-13712-ES-20020318

Kit Location: <http://ftp1.support.compaq.com/public/unix/v5.1/>

Tru64 UNIX 5.1A

PREREQUISITE: Tru64 UNIX 5.1A with PK1 (BL1) installed

ERP Kit Name: T64V51AB1-C0014802-13710-ES-20020318

Kit Location: <http://ftp1.support.compaq.com/public/unix/v5.1a/>

MD5 and SHA1 checksums are available in the public patch notice for the ERP kits. You can find information on how to verify MD5 and SHA1 checksums at:

<http://www.support.compaq.com/patches/whats-new.shtml>

Compaq Insight Management Suite:

(ProLiant running industry standard operating systems including Windows 2000, NetWare, Linux, etc)

The Compaq Insight Management Suite utilizes SNMP as a primary communications method. Fixes to the operating systems affected will be provided by the vendors involved. Check

<http://www.compaq.com/manage/security> the most up-to-date information.

Deskpro, Professional Workstation, Armada, Evo:

The Deskpro, Professional Workstation, Armada, Evo (Microsoft operating systems including Windows XP, Windows 2000, Windows 98, and Windows 95) Compaq Management Agents for Clients utilizes SNMP as an optional communications method.

Fixes to the operating systems affected will be provided by Microsoft. Check www.microsoft.com/technet/security/bulletin/MS02-006.asp for the most up-to-date information.

Compaq SANworks Management Appliance:

The SANworks management appliance is essentially a Compaq server and our recommended configuration does not have it connected directly to the internet. Therefore, it is less exposed than other servers to external SNMP security attacks. However, the appliance is susceptible to SNMP security attacks from inside the firewall that could result in the graceful termination of some storage management applications on the appliance.

Compaq will provide a patch to the appliance as soon as possible.

COMPAQ STORAGEWORKS PRODUCTS:

UPDATE: 08 MARCH, 2002

The following Compaq StorageWorks products have Ethernet connections that may potentially be exposed to the SNMPv1 vulnerability:

Compaq StorageWorks SAN Switch 8, 8-EL, 16, 16-EL, 2/16, Integrated 32 or 64 Port
Compaq StorageWorks SAN Director 64
Compaq StorageWorks Modular Data Router
Compaq StorageWorks 12 Port Fibre Channel Managed Hub
Compaq StorageWorks 20/40 GB 8 Cassette AutoLoader

RESOLUTION:

Compaq StorageWorks SAN Switch 8, 8-EL, 16, 16-EL, 2/16, Integrated 32 or 64 Port:
There are currently no known issues related to vulnerability notes VU#854306 or VU#107186 with these products. They have passed all validation tests conducted to date.

Compaq StorageWorks SAN Director 64:

This product has been evaluated with a SNMP based test program that attempts to overload the director with SNMP traffic such as GET, Set and Get Next commands. No problems were found in this testing. Additionally, Compaq is in the process of evaluating the details of the SNMP implementation in this product. Any problems identified that are determined to pose a risk to customer operations will be documented and addressed in future maintenance releases. Note that the advisory documented two areas of vulnerability. One area involves Trap handling on the part of SNMP Management components, and the other area involves the processing of GET, Set and Get Next commands on the part of SNMP Agent components. The director implements only the SNMP Agent components, so none of the problems related to Trap handling apply. Also, the SNMP Agent on the director management server is disabled by default. No SNMP messages are processed by the management server unless the systems administrator has explicitly enabled the SNMP Agent. On the director itself, the SNMP Agent is enabled by default, but for read access only.

Compaq StorageWorks Modular Data Router:

The potential vulnerability has to do with SNMP Set commands. The only Set command the MDR allows is to set the trap address.

Compaq StorageWorks 12 Port Fibre Channel Managed Hub:

Compaq is in the process of evaluating the SNMP implementation in this product.

Compaq StorageWorks 20/40 GB 8 Cassette AutoLoader:

Compaq is in the process of evaluating the SNMP implementation in this product.

COMPAQ/MICROCOM PRODUCTS:

UPDATE: MARCH 08, 2002

Microcom Access Integrator (All Versions)

Compaq-Microcom 6000 Series Remote Access Concentrators(All Versions)

Both products use SNMPv1 protocol as the transport for system management, either through expressWATCH, or third party SNMP clients. These products are normally managed over the LAN by clients using IP ports UDP 161 for SNMP and UDP 162 for SNMP Traps. The SNMP agents integrated in these products cannot be disabled. Access to the system

via the PRI, T1 or analog modules do not present a security risk related to SNMPv1.

Incursions may result in instability of the system requiring a hard reset of one or more of the systems modules, which will result in temporary loss of connectivity to dial in clients. Users will be able to reconnect after the systems has reset.

RECOMMENDATIONS:

Compaq recommends the following precautions in accordance with good general networking administration practices.

1. Apply perimeter filtering to SNMP traffic. Upstream internet routers, or Firewall should be configured to filter UDP ports 161 and 162.

2. Compaq has always recommended that the associated engines contained in the CM6000 Series reside on an internal network using a non-routable private addressing scheme.

3. The system should not be managed over the internet or an non secure LAN.

Microcom ISPorte (All Versions)
Compaq Microcom 4000 concentrator

These products make very limited use of the SNMPv1 protocol on the Ethernet portion of their PRI/T1 modules. In the limited number of installations where digital calls are being tunneled to NT servers on the connected LAN, there is a potential for SNMP packets to reach the PRI/T1 card through it's Ethernet port. Access to the system via the analog modem modules do not present security risk related to SNMPv1.

Incursions may result in instability of the PRI/T1 card, resulting in a loss of connectivity for dial in users. A hard reset is the only way to correct these failure, but a hard reset will also disconnect all remaining users. Users will be able to reconnect after the system resets.

RECOMMENDATIONS:

Compaq recommends the following precautions in accordance with good general networking administration practices.

1. Apply perimeter filtering to SNMP traffic. Upstream internet routers should be configured to filter UDP ports 161 and 162.
2. If the system is being used for analog dial in access only, it should not be connected to the LAN via the Ethernet port on the PRI/T1 card.

Microcom SNMP HDMS+ System (Version 1.3.1)

The great majority of HDMS+ systems installed do not have SNMP capabilities and are therefore not at risk. These systems can be identified by the absence of a 10baseT connector on the rear of the controller card.

A limited number of SNMP HDMS+ systems were produced, this product uses SNMPv1 protocol as the transport for system management. Management clients can include either expressWATCH, or third party SNMP clients.

The product can be managed over the LAN by clients using IP ports UDP 161 for SNMP and UDP 162 for SNMP Traps, or through a serial RS232 port using SLIP. The SNMP agents integrated in these products cannot be disabled. Access to the system via the analog modem modules do not present security risk related to SNMPv1.

Incursions may result in instability of the systems management controller, which may require a hard reset. The reset of this controller may result in a temporary loss of connectivity for dial in users. Dial in users will be able to reconnect after the system has reset.

RECOMMENDATIONS:

Compaq recommends the following precautions in accordance with good general networking administration practices.

1. Apply perimeter filtering to SNMP traffic. Upstream internet routers or firewalls should be configured to filter UDP ports 161 and 162.
2. The system should not be managed over the internet.
3. The system should not be managed over a non secure LAN.

Direct management via a serial RS232 SLIP connection would be recommended.

For assistance or clarification on any of the recommendation for Compaq/Microcom products, please call 01-800-652-6672 and from the menu select 2,3,1 then enter routing code 1851

NOTE: Many systems operate behind firewalls and would normally implement SNMP blocking for SNMP as standard procedure. Based on SNMP blocking and ingress/egress filtering, the potential Security vulnerability may only be exploited by users who have access to your local security domain, therefore the risk is diminished.

SUPPORT: This advisory bulletin will be updated for the various products requiring patches and individual patch notifications will be done through standard "patch notification" procedures for those products. For further information, contact your normal Compaq Support channel.

SUBSCRIBE: To subscribe to automatically receive future Security Advisories from the Compaq's Software Security Response Team via electronic mail: <http://www.support.compaq.com/patches/mailling-list.shtml>

REPORT: To report a potential security vulnerability with any Compaq supported product, send email <mailto:security-ssrt@compaq.com> or <mailto:sec-alert@compaq.com>

Compaq appreciates your cooperation and patience. As always, Compaq urges you to periodically review your system management and security procedures. Compaq will continue to review and enhance the security features of its products and work with our customers to maintain and improve the security and integrity of their systems.

"Compaq is broadly distributing this Security Bulletin in order to bring to the attention of users of the affected Compaq products the important security information contained in this Bulletin. Compaq recommends that all users determine the applicability of this information to their individual situations and take appropriate action. Compaq does not warrant that this information is necessarily accurate or complete for all user situations and, consequently, Compaq will not be responsible for any damages resulting from user's use or disregard of the information provided in this

Bulletin."

Copyright 2002 Compaq Information Technologies Group, L.P.
Compaq shall not be liable for technical or editorial errors
or omissions contained herein. The information in this document
is subject to change without notice. Compaq and the names of
Compaq products referenced herein are, either, trademarks
and/or service marks or registered trademarks and/or service
marks of Compaq Information Technologies Group, L.P. Other product
and company names mentioned herein may be trademarks and/or service
marks of their respective owners.

-----BEGIN PGP SIGNATURE-----

Version: PGP 7.0.1

iQA/AwUBPLQ7jznTu2ckvbFuEQLuTwCgrJV3CBEwYiFEbWsCF0mbHBRVc/oAoNcI
1KxCsylGTohymyn9t4kbuR/C
=F6B1

-----END PGP SIGNATURE-----

Computer Associates

Computer Associates has confirmed Unicenter vulnerability to the SNMP advisory identified by CERT notification reference [VU#107186 & VU#854306] and OUSPG#0100. We have produced corrective maintenance to address these vulnerabilities, which is in the process of publication for all applicable releases / platforms and will be offered through the CA Support site. Please contact our Technical Support organization for information regarding availability / applicability for your specific configuration(s).

COMTEK Services, Inc.

In reference to your notification regarding [VU#617947] [OUSPG#0100], vulnerabilities in COMTEK Services' SNMP products are as follows:

NMServer for AS/400 is not an SNMP master and is therefore not vulnerable. However this product requires the use of the AS/400 SNMP master agent supplied by IBM. Please refer to IBM for statements of vulnerabilities for the AS/400 SNMP master agent.

NMServer for OpenVMS has been tested and has shown to be vulnerable. COMTEK Services has released a new version (version 3.5) of this product that includes a fix for this problem. Contact COMTEK Services support@comtekservices.com to arrange to download the new version.

NMServer for VOS has not as yet been tested; vulnerability of this agent is unknown. Contact support@comtekservices.com for further information on the testing schedule of the VOS product.

Concord Communications, Inc.

Concord's eHealth Console product has some vulnerabilities to the OUSPG test suite. Patches are available.

Concord's SystemEDGE agent has been tested and is not vulnerable on Unix platforms. Under Windows, it is a sub-agent of the Windows SNNMP agent, and therefore the Windows hot fixes should be applied. SystemEDGE is not vulnerable on Win2K and XP with Microsoft's hot fixes.

Please see this page on Concord's web site for more detail and for patch availability:
<http://www.concord.com/certadvisory.shtml>

Conectiva

The ucd-snmp package from Conectiva Linux 5.0, 5.1, 6.0, 7.0, "ferramentas gráficas" and "ecommerce" are affected by this vulnerability. Previous Conectiva Linux are also affected, but they are no longer supported and no update will be provided for them.

New packages will be provided shortly and will be announced to our mailing lists and updates website (<http://distro.conectiva.com.br/atualizacoes/>).

Error! Hyperlink reference not valid.

Controlware GmbH

In order to determine the impact of these vulnerabilities, Controlware immediately started extensive testing of the effected products. The results of these tests can be viewed on the Website.

Corsaire Limited

Corsaire Limited response to SNMP Vulnerability Test Suite (CERT Advisory CA-2002-03)

Corsaire Limited have analysed the Secure Technical Assistance Centre (STAC) SNMP agent software that is used as part of their managed services solution and can confirm that the agent is not susceptible to any of the vulnerabilities reported.

The STAC SNMP agent software has been entirely developed in-house and does not rely on any third-party libraries. Probing by the PROTOS test suite is correctly recognised as malformed packets and reported as such within the audit trail.

Further information is available from <http://www.corsaire.com>

Covalent Technologies

Covalent Technologies has tested the Enterprise Ready Server, Managed Server, and Covalent Conductor SNMP module according to recommendations issued by CERT, and has found no security vulnerabilities associated with Advisory CA-2002-03.

Cray Inc.

Cray, Inc. had opened spr 721879 to track this problem. At this time, Cray suggests that Unicos and Unicos/mk sites disable the SNMP daemon.

CSCare, Inc.

As a result of this advisory, CSCare has conducted extensive testing of its products. We have determined that exploiting these vulnerabilities can interfere with the normal operation of Trap Console 1.4b. Results have not indicated any vulnerability that will allow an attacker to gain access to the host computer. It has been determined that Active SNMP 2.0b is not vulnerable.

CSCare has released Trap Console 1.4c update on March 5, 2002. This release containing fixes for all known vulnerabilities is now available for download at <http://www.cscare.com/TrapConsole>.

For more information, please feel free to contact CSCare by email at info@cscare.com or by phone at 408-490-2736.

Dart Communications

In response to CERT® Advisory CA-2002-03, the PowerTCP SNMP Tool has been reviewed and found vulnerable for issue VU#854306 and VU#107186. To address these issues, an update of the PowerTCP SNMP Tool will be released on February 28th, 2002. Details of the specific problems found and the methods used to address these vulnerabilities will be included in the PowerTCP Release History at <http://www.dart.com/downloads/update.txt>. If you have any questions concerning PowerTCP SNMP security vulnerabilities, please contact Dart Communications at support@dart.com.

Dartware, LLC

Dartware, LLC (www.dartware.com) supplies two products that use SNMPv1 in a manager role, InterMapper and SNMP Watcher. These products are not vulnerable to the SNMP vulnerability described in [VU#854306 and VU#107186]. This statement applies to all present and past versions of these two software packages.

In addition, our port of net-snmp to MacOS X has been updated to version 4.2.2, and is not susceptible to this attack. More information is available from <http://www.dartware.com/net-snmp/>

Dell

Title

Dell Response to CERT® Advisory CA-2002-03 Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol (SNMP)

Audience

For worldwide distribution provided that the contents are not altered in any way.

Released

April 8, 2002

Updated

April 19, 2002 (Updated the Dell PowerVault section regarding PowerVault 701N and PowerVault 705N)

Reference

CERT Advisory CA-2002-03 - <http://www.cert.org/advisories/CA-2002-03.html>

Overview

The CERT/CC released an industry-wide SNMP advisory on February 12, 2002. An SNMPv1 test suite provided by the Oulu University Secure Programming Group (OUSPG) has been found to adversely affect many SNMPv1 implementations, causing the potential for “unauthorized privileged access”, “denial-of-service attacks” and general unstable behavior.

Potential Impact

Dell PowerEdge

Dell OpenManage

Dell PowerVault

Dell PowerApp

Dell PowerConnect

Dell PowerEdge, Dell OpenManage

Dell PowerEdge servers running Dell OpenManage software utilize SNMPv1, however this software makes use of the operating system’s master SNMP agent. After applying the appropriate update(s) from the operating system manufacturer, Dell SNMP agents are not affected.

Solution: Apply the appropriate update(s) provided by the operating system vendor. For more information, [click here](#).

Dell PowerVault

The following Dell PowerVault storage systems have been found vulnerable to the OUSPG SNMPv1 test suite:

Dell PowerVault 701N

Dell PowerVault 705N

Solution: These devices require an update from Dell.

The Dell PowerVault Assist utility that is required to update both PowerVault 701N and

PowerVault 705N devices can be found here.

The updated image for both the PowerVault 701N and PowerVault 705N devices can be found here.

Dell PowerApp

The following Dell PowerApp appliance has been found vulnerable to the OUSPG SNMPv1 test suite:

Dell PowerApp 220 (Dell PowerApp.BIG-IP)

Solution: This device requires an update from Dell.

Information regarding the update for *non-encrypted* devices can be found here.

Information regarding the update for *encrypted* devices can be found here.

Dell PowerConnect

All Dell PowerConnect devices successfully passed the test cases provided by the OUSPG SNMPv1 test suite.

Operating System Vendor Information

The following Dell supported operating system vendors have released information regarding their SNMPv1 vulnerabilities:

Microsoft®

<http://www.microsoft.com/technet/security/bulletin/MS02-006.asp>

Novell®

<http://support.novell.com/servlet/tidfinder/2961546>

Red Hat®

<http://www.redhat.com/support/errata/RHSA-2001-163.html>

Dell Computer Corporation has provided this advisory bulletin in response to the concerns raised by OUSPG and to provide information to users of Dell systems regarding its SNMP implementation. Dell recommends that user's review this information and determine its applicability to their individual situations. In addition, Dell does not provide any warranty as to the accuracy or completeness of this information and will not be liable for damages that may result from usage or disregard of the information provided. The information provided is subject to change. For further information and related updates, please contact your standard Dell support channel. Dell retains ownership of its trademarks and service marks as well as the information contained in this advisory bulletin.

Digital Networks

Digital Networks is addressing the vulnerabilities identified in this advisory. The latest information on the affect of this vulnerability on Digital Networks products as well as any remedial software patches can be found at <http://www.digitalnetworks.net/support>.

D-Link Systems, Inc.

D-Link has tested our DES-3226, DES-3326, DES-3624i and DES-6000 products and determined that these products are not susceptible to the SNMP vulnerability issue. Since all D-Link products with SNMP agent use the same code base, D-Link has concluded that all of our products do not have the SNMP vulnerability issue. However, we continue to evaluate and investigate all D-Link products implemented with SNMP agent. Upon completion of our evaluation, D-Link will provide and post an update with our thorough test results.

DMH Software

DMH Software applied the OULU University test suite to its various portable snmp-agent products: SNMPv1, SNMPv2c and SNMPv3.

We found that the following or later releases of DMH portable snmp-agent products are NOT vulnerable to CERT vulnerability advisory VU#854306 (Multiple vulnerabilities in SNMPv1 request handling)

- (1) SNMPv1 Agent version - 2.0.9.1
- (2) SNMPv2c Agent version - 3.0.5.3
- (3) SNMPv3 Agent version - 4.0.8.2

The above releases, or newer releases, are currently available to our customers. We strongly recommend our customers to contact us to obtain an upgrade and update their source code.

Please note that we received notes from some of our customers who reported that previous releases of DMH snmp-agent products were tested and found not vulnerable to VU#107186. Nevertheless we recommend an upgrade to the recent releases.

Efficient Networks, Inc.

Efficient Networks, Inc. has reviewed CERT Advisory CA-2002-03 and is performing the recommended tests to determine if its products are impacted. The following products do not have SNMP management capabilities and are not affected: SpeedStream 1000, 2000, 3000, 4000, 5200, and

5300 series devices, as well as the 5667 bridge product. Testing is still in progress on other Efficient Networks' products. Efficient Networks will continue to update its statement on this site as additional information becomes available.

EnGarde Secure Linux

EnGarde Secure Linux did not ship any SNMP packages in version 1.0.1 of our distribution, so we are not vulnerable to either bug.

Enterasys

On 12-February-2002, CERT (<http://www.cert.org>) announced serious vulnerabilities in the SNMP implementations of virtually every networking vendor's equipment. These vulnerabilities were discovered by a Finnish research group known as OUSPG, associated with Oulu University, and are documented in advisory CA-2002-03.

These vulnerabilities exist in all versions of SNMP (v1/v2c/v3) and can be used to cause SNMP implementations to behave in an unpredictable manner, resulting in denials of service or system failures.

Given the serious nature of these vulnerabilities, Enterasys is testing our product line to determine which products are affected. Patches for affected products will be made available to our customers. Please check the Enterasys Support web site periodically for further details and patch information.

Until these patches become available, Enterasys recommends that the following steps be taken to help reduce exposure to these vulnerabilities.

- Disable SNMP from interfaces through which SNMP commands should not be received, such as those providing connection from the Internet or Extranets.
- Use Access Control Lists at the access edge to prevent SNMP traffic from unauthorized internal hosts from entering the network.
- Use management VLANs or out-of-band management to contain SNMP traffic and multicasts. These do not prevent an attacker from exploiting these vulnerabilities, but they may make it more difficult to initiate the attacks.
- Enable 802.1X port-locking and RADIUS to prevent unauthenticated users from attaching to the network.
- Use NetSight Policy Manager to automatically restrict the use of SNMP to authenticated, SNMP-authorized personnel.
- Update Dragon IDS signatures to help identify when these attacks are being used.

Entrada Networks

This is in reference to you notification regarding VU#854306, VU#107186, and OUSPG#0100. Entrada Networks has reproduced this behavior and coded a software release enhancement for the

affected products which is currently in regression testing within Entrada Networks' Quality Assurance organization. The release of Entrada Networks software enhancement addressing the behavior outlined in VU#854306, VU#107186, and OUSPG#0100 will be available to Entrada Networks, Sync Research, and Rixon Networks customers with Software Subscription Service on a request basis, no later than April 15, 2002.

Entrada Networks has also produced a document discussing the alternative workarounds or configuration options to address the behavior outlined in VU#854306, VU#107186, and OUSPG#0100. This document is also available on request from customers. Please contact the Technical Support organization at 800-331-8669 for more information.

Entrada Networks is providing the statement below as a response to be included in your vendor's statement section on SNMP CERT Alert 2002-03.

Entrada Networks Sync Research, Inc. and Rixon Networks, Inc., (both are companies of Entrada Networks)

Entrada Networks, through the companies of Sync Research, Inc. and Rixon Networks, has confirmed vulnerability to the SNMP advisory identified by CERT notification reference [VU#107186 & VU#854306] and OUSPG#0100.

Sync Research also manufactures and supports products formerly manufactured by Tylink, Inc. and Osicom, Inc.
Rixon Networks, Inc. also manufactures and supports products formerly manufactured by Osicom, Inc.

Entrada Networks has run all the test cases found in the PROTOS test-suite, c06snmpv1:

1. c06-snmpv1-req-app-pr1.jar
2. c06-snmpv1-req-enc-pr1.jar
3. c06-snmpv1-trap-app-pr1.jar
4. c06-snmpv1-trap-enc-pr1.jar

The tests were run with standard delay time between the requests (100ms).

Entrada Networks, through their companies of Sync Research and Rixon Networks, supplies a broad range of networking products, some of which are affected by the SNMP vulnerabilities identified by CERT Coordination Center. The manner, in which, they are affected and the actions required to avoid being impacted by exploitation of these vulnerabilities varies from product to product.

Entrada Networks customers may contact our Technical Support Center via either telephone 800-331-8669 or via email: <mailto:support@sync.com> for

additional information, especially regarding their availability of the latest enhanced code releases addressing the SNMP vulnerabilities.

The tests that were run apply to the following Entrada Networks, Sync Research, and Rixon Networks products.

The Sync Research FRADs (3600,3700, 4200, and 4300 series), the Tylink FRAPs (D-FRAP, M-FRAP, S-FRAP, T-FRAP), Sync Research management platform (Envisage for Windows and Envisage for UNIX) and the Osicom Routermate series.

The software tested on these products was the latest software releases that are generally available.

Entrada Networks is in the process of creating a publication for all applicable releases / platforms and will be offering this publication through the Entrada Networks Support site at < <http://www.entradanetworks.com>> or the Sync Research, Inc. site at < <http://www.sync.com>> at a future date.

Please contact our Technical Support organization for information regarding availability / applicability for your specific configurations.

Following is a list of companies whose products are addressed by this preliminary response:

Sync Research, Inc. (see Entrada Networks)
Osicom, Inc. (see Entrada Networks)
Rixon Networks, Inc. (see Entrada Networks)
Torrey Pines Networks, Inc. (see Entrada Networks)
Tylink, Inc. (see Entrada Networks)

Equinox Systems

This is in reference to the CERT Advisory CA-2002-03 addressing potential security vulnerabilities that exist in network devices using SNMPv1 as the management protocol. Equinox has determined that exploitation of these vulnerabilities may interfere with normal operation of our ESP serial hub through malicious use of the management interfaces provided for its Equiview Plus application. We are evaluating the impact on the ESP and will release appropriate fixes if necessary. In the interim, Equinox recommends the following mitigation procedures.

In most network environments, firewalls are deployed to prohibit externally originating SNMP traffic and both detect and prevent Denial of Service attacks. Since the ESP does not currently allow for disabling of SNMP, it is recommended that this device be operated in a secure environment in conjunction with the following SNMP network security safeguards:

1. Filter SNMP access to managed devices to ensure the traffic originates from known management systems
2. Use upstream firewall/access lists to deny access to the SNMP agents accessible on the network
3. Use access profiles to deny SNMP access to unknown users
4. Use dedicated management VLANs or out-of-band management to contain SNMP traffic and multicasts
5. Change the default community strings

Equinix will continue to address potential security problems across its product line and provide patches as circumstances dictate.

e-Security, Inc.

e-Security Advisory:

SNMPv1 Request and Trap Handling Vulnerabilities

Revision 1.0

Release Date: March 14, 2002

Summary

On February 12, 2002 the CERT®/CC released an advisory related to security vulnerabilities that may exist in network devices using SNMPv1 as the management protocol. The vulnerabilities may allow unauthorized privileged access, denial of service attacks, or cause unstable behavior. In response to this advisory, "CERT® Advisory CA-2002-03 Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol (SNMP)", e-Security began executing the tests that elicit these vulnerabilities for all e-Security products.

The issue centers on the SNMP library that we use in our products to communicate in SNMP versions 1,2 & 3. Currently, e-Security uses SNMP Research's Emanate 15.2.7 on with our agents (e-Wizard and eSAW) and UC Davis 4.0.1 with our control center (e-Sentinel and OeSP).

Preliminary test results have indicated that e-Sentinel, e-Wizard, OeSP, and e-SAW products exhibited the vulnerabilities in the CERT® Advisory.

Though we were affected with the vulnerabilities in our code, note this should not be viewed as a negative statement on SNMP protocol, as the latest packages from UC Davis and SNMP Research are not vulnerable to these exploits.

Solution

e-Security has applied the PROTOS c06-SNMPv1 test suite to all e-Security products and has released patches to eliminate these vulnerabilities. Our patches address e-Security products through v.3.1. Future releases of e-Security products will utilize the latest packages from UC Davis and SNMP Research which have resolved these vulnerabilities.

e-Security also recommends considering one or more of the following solutions to minimize your network's potential exposure to these vulnerabilities:

- Ingress filtering
- Egress filtering
- Filter SNMP traffic from non-authorized internal hosts
- Change default community strings

For Further Information

Contact e-Security Customer Support at 1-800-474-3131, or you can e-mail us at support@esecurityinc.com.

Evidian Inc.

[VU#854306](#)

This advisory is not applicable to OpenMaster for Telecom as it is a management system and not an agent. As a management system, OpenMaster for Telecom processes subsequent SNMP responses or send SNMP requests but doesn't process any SNMP requests.

[VU#107186](#)

Evidian will issue a bulletin regarding this advisory once we have completed the investigation.

Extreme Networks

Extreme Networks has identified the vulnerability outlined in this CERT Advisory CA-2002-03 and is in addressing the issue. A technical advisory has been released. Please go to the following web site for information: <http://www.extremenetworks.com/support/techsupport.asp>.

F5 Networks

All versions of BIG-IP, 3-DNS, GLOBAL-SITE and EDGE-FX are vulnerable if the SNMP agent is enabled. Most versions have the SNMP agent enabled by default. Patches are available for all affected versions.

SEE-IT is not affected by this vulnerability.

If a customer is unable to install the patch, the SNMP service may be disabled. Below are instructions for obtaining patches and for disabling the SNMP service for each vulnerable product.

BIG-IP

A patch exists to correct this problem. Please see <http://tech.f5.com/home/bigip/solutions/security/sol1622.html>.

Alternatively, you can simply disable the SNMP service using the instructions below:

1. Log in to the BIG-IP Configuration utility.
2. Navigate to the SNMP section. For version 4.0 and above this is a tab under **System Administration**.
3. De-select the Enable box at the top of the screen and click the **Apply** button.

This will disable the SNMP service on BIG-IP.

3-DNS

A patch exists to correct this problem. Please see <http://tech.f5.com/home/3dns/solutions/security/sol1624.html> .

Alternatively, you can simply disable the SNMP service using the instructions below:

1. Log in to the 3-DNS Configuration utility.
2. Navigate to the SNMP section. This is the tab under **3-DNS Sync** .
3. De-select the **Enable** box at the top of the screen and click the Apply button.
4. Log in to the Command Line Interface of the 3-DNS.
5. Run the following command:

```
kill -9 `ps -ax | grep snmpd | awk '{print $1}'`
```

This will disable the SNMP service on 3-DNS.

GLOBAL-SITE

A patch exists to correct this problem. Please see <http://tech.f5.com/home/globalsite/solutions/security/sol1626.html>.

Alternatively, you can simply disable the SNMP service using the instructions below:

GLOBAL-SITE version 2.2

To disable the SNMP agent for GLOBAL-SITE version 2.2, type the following command from the command prompt:

```
ITCMconsole service snmpd stop
```

This command stops the **snmpd** agent.

```
ITCMconsole service snmpd disable
```

This command disables **snmpd** so it does not start again at the next boot.

To verify the status of **snmpd**, enter the following command:

```
ITCMconsole show snmpd status
```

GLOBAL-SITE version 2.1PTF-01 and earlier:

On versions 2.1 PTF-01 and earlier, **snmpd** is not running by default so the GLOBAL-SITE Controller should not be affected. However, if you have enabled **snmpd** manually, you should disable it.

EDGE-FX

A patch exists to correct this problem. Please see <http://tech.f5.com/home/edgefx/solutions/security/sol1625.html> .

Alternatively, you can simply disable the SNMP service using the instructions below:

There are three SNMP daemons running on the cache. By default, the EDGE-FX Cache runs the **snmpd**, the **edgefxsnmpd**, and Inktomi's **snmpdm** .

Disabling snmpd and edgefxsnmpd

To disable and stop the SNMP agents, you should use the ITCMconsole. Type the following commands from the command prompt:

```
ITCMconsole service snmpd stop
```

This command stops the **snmpd** agent.

```
ITCMconsole service snmpd disable
```

This command disables **snmpd** so it does not start again at the next boot.

To verify the status of **snmpd**, enter the following command:

```
ITCMconsole show snmpd status
```

Once the **snmpd** and **edgefxsnmpd** daemons are disabled, no other snmp traffic will be accepted.

Disabling snmpdm

The **snmpdm** agent, is also enabled by default. This Inktomi specific agent can be disabled or killed. In order to avoid traffic server anomalies, you should not kill this this daemon.

According to CERT® Advisory CA-2002-03 :

"Inktomi Corporation does not believe our [Inktomi] CDS product is vulnerable. Vulnerability would stem from the use of SNMP Research software in the CDS product. However, SNMP Research has stated that their product Emanate, versions 15.x and higher, is not vulnerable. As Inktomi's CDS uses Emanate 15.3, we [Inktomi] conclude that CDS is not vulnerable."

Inktomi's CDS contains the same Traffic Server that EDGE-FX utilizes, which contains the Emanate 15.3 daemon (**snmpdm**).

If you still want to kill this SNMP agent, you can use the Configuration utility or the command line.

To disable the SNMP agent from the Configuration utility:

1. From your browser, access the Configuration utility (refer to Accessing the Configuration utility).
2. On the Configure tab, click the **Server** button.
3. Scroll to the SNMP section of the Server Basics page.
4. Click the **SNMP Agent Off** radio button.
5. Click the **Make These Changes** button.

To disable the SNMP agent manually:

1. In a text editor, open the **records.config** file located in the EDGE-FX Cache's **/config/traffic_server/config** directory.
2. Edit the following variable:
proxy.config.snmp.master_agent_enabled

- Set this variable to **0** to disable SNMP on the EDGE-FX Cache node.
3. Save and close the **records.config** file.
 4. Make the **/usr/local/cache/bin** directory the working directory and run the following command to apply the configuration changes.

```
./traffic_line -x
```

Note: you can also use the following command to restart the traffic_server: `start_traffic_server`.

SEE-IT

It has been determined that SEE-IT is not vulnerable.

Fluke Corporation

Fluke Networks' response to CERT Advisory 2002-03

The CERT® Coordination Center recently announced that numerous vulnerabilities have been reported in multiple vendors' SNMP implementations. For your information, Fluke Networks has created the following Q&A which includes a tutorial, Using Fluke Networks products to manage SNMP risk on your network.

Q&A

What is the actual risk?

The impact of the vulnerability is different for each vendor and their own products. For SNMP agents and Trap listeners running on network operating systems, some attacks could bypass system security controls. Overall, most attacks resulted in a “denial-of-service” in which the entire product or portions of the product stopped working properly.

Which Fluke Networks products are affected?

Fluke Networks has tested its products that listen for SNMP Traps or contain an internal SNMP agent. It has been discovered that some circumstances exist that could potentially cause a “denial-of-service” condition for a Fluke Networks product, forcing the product to “hang” or reboot. However, this situation would only affect Fluke Networks products and would not compromise our customers' networks.

Fluke Networks products that could be affected include the OptiView™

Integrated Network Analyzer, the OptiView™ Workgroup Analyzer and the OptiView™ Link Analyzer.

As of this writing, there have been no known "denial-of-service" incidents reported with Fluke Networks products. To reiterate, should such an event occur involving a Fluke Networks product, this would not affect the operation of customers' networks or any of their network infrastructures. Nor would there be any risk of anyone externally gaining access to customer data.

Future action

At this time, we plan to resolve all known vulnerabilities in the next scheduled software update for the affected products. Customers who participate in the Gold Priority Support program will be eligible to receive these updates as part of their membership. Customers who do not participate in this program should contact our Technical Assistance Center (TAC) at 1-800-638-3497 (North America) or +1-425-446-4519 (Outside North America).

Recommendations

We recommend the following "best practices" to reduce the potential risk of SNMP related attacks:

1. Ensure that you external firewalls deny all incoming SNMP traffic.
2. Change the default community strings for all SNMP devices. Audit your network for devices using the community strings of "public" and "private" as well as for those other community strings that are set by default by equipment manufacturers.
3. Analyze SNMP traffic for patterns of attack.

Tutorial: Using Fluke Networks products to manage this risk on your network

1. Identify SNMP agents on the network

The OptiView Integrated Network Analyzer and OptiView Workgroup Analyzer have the capability of discovering all devices within a broadcast domain that are SNMP enabled.

On the Setup/Security screen, configure all known and old community strings making sure you include strings such as "public", "private" and "security".

Re-run the tests by selecting the "Rerun Test" tab.

Select the "Discovery" tab and then select the SNMP Agents category in the left hand pane. The resulting display shows all SNMP agents discovered by the test.

2. Test your firewall for filtering SNMP traffic

From a LAN segment outside your firewall, use the OptiView Integrated Network Analyzer to query known SNMP agents on the protected side of your network. After the "Network-Under-Test" interface has a proper IP configuration, enter the IP address of a known SNMP agent on the Tools screen.

Note: Using Fluke Networks' Protocol Expert™ on the protected side of your firewall, allows you to see if the firewall is denying any and all SNMP traffic from flowing through the firewall as well as preventing SNMP responses from leaving your network.

Using two OptiView Analyzers, one on either side of the firewall, can be used to easily check this condition. Use the Packet Capture and Statistics feature to ensure that no SNMP traffic is flowing in from outside of the firewall.

3. Analyze network patterns for SNMP attacks

Using the OptiView Integrated Network Analyzer, the OptiView Workgroup Analyzer or the OptiView Link Analyzer, a combination of packet capture and protocol statistics can be used to gather evidence of an SNMP attack.

Select the "Top Hosts" tab to look for nodes that should not be sending SNMP queries. Select the "Top Conversations" to check for unusual Conversation Pairs within the SNMP traffic.

Fluke Networks' Copper and Fiber taps can be used to access switch-to-switch links and the Switch-TAP™ capability of the OptiView™ Inspector Console can be used to program the mirror ports of a variety of switches.

For more information

For questions, concerns or more information, please contact the Fluke Networks TAC at 1-800-638-3497 (North America), +1-425-446-4519 (outside North America) or email us at: nettech@flukenetworks.com.

Foundry Networks, Inc.

According to testing completed by Foundry engineering using the stress tools recommended by CERT, we determined that NO Foundry devices are affected by any known SNMP security issue. All of Foundry's products use the same SNMP engine with varying SNMP versions (v1, v2c, and v3), and all SNMP versions have been tested.

We are extremely appreciative to CERT's help during our testing period, and would like to wholeheartedly thank everyone involved.

FreeBSD

FreeBSD does not include any SNMP software by default, and so is not vulnerable. However, the FreeBSD Ports Collection contains the UCD-SNMP / NET-SNMP package. Package versions prior to ucd-snmp-4.2.3 are vulnerable. The upcoming FreeBSD 4.5 release will ship the corrected version of the UCD-SNMP / NET-SNMP package. In addition, the corrected version of the packages is available from the FreeBSD mirrors.

FreeBSD has issued the following FreeBSD Security Advisory regarding the UCD-SNMP / NET-SNMP package:

<ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-02:11.snmp.asc>.

Future Communications Software

FutureSoft has tested its SNMP Product FutureSoftSNMP Release 5.0.1.0 according to the recommendations issued by CERT, and has found no security vulnerabilities associated with Advisory CA-2002-03 (Multiple Vulnerabilities in Many Implementations of SNMP).

General DataComm

General DataComm Advisory Bulletin

<http://www.gdc.com/products/bulletin.shtml>

Ref: CERT Advisory CA-2002-03

Multiple Vulnerabilities in Many Implementations of Simple Network Management Protocol (SNMP)

GDC TEAM SNMP

The GDC TEAM applications use the HP OpenView NNM SNMP protocol stack for its SNMP network management communication to its SpectraComm Manager (SCM) card. The SCM contains an SNMP proxy agent.

Recommendations:

1. The SCM does not have a default read/write community name of "private" which makes it less

susceptible for hackers to change device configurations or taking down the management or data network. The SCM does have a default read only community name of "public". The customer is advised to change this.

2. The major GDC network management customers usually use a separate private LAN for their management traffic to eliminate the exposure to outside illegal entry.

3. Please read below, obtain and install the HP HPOV patches from the listed sites.

HP HPOV NNM (Network Node Manager)

Some problems were found in NNM product were related to trap handling. Patches in process. Watch for the associated HP Security Bulletin.

HP-UX Systems running snmpd or OPENVIEW

The following patches are available now:

PHSS_26137 s700_800 10.20 OV EMANATE14.2 Agent Consolidated Patch
PHSS_26138 s700_800 11.X OV EMANATE14.2 Agent Consolidated Patch

PSOV_03087 EMANATE Release 14.2 Solaris 2.X Agent Consolidated Patch

All three patches are available from:

<http://support.openview.hp.com/cpe/patches/>

In addition PHSS_26137 and PHSS_26138 will soon be available from:

<http://itrc.hp.com>

NOTE: The patches are labeled OV(Open View). However, the patches are also applicable to systems that are not running Open View.

Any HP-UX 10.X or 11.X system running snmpd or snmpdm is vulnerable. To determine if your HP-UX system has snmpd or snmpdm installed:

```
swlist -l file | grep snmpd
```

If a patch is not available for your platform or you cannot install an available patch, snmpd and

snmpdm can be disabled by removing their entries from /etc/services and removing the execute permissions from /usr/sbin/snmpd and /usr/sbin/snmpdm.

Hewlett-Packard Company

HP Support Information Digests

o Security Bulletin Digest Split

The security bulletins digest has been split into multiple digests based on the operating system (HP-UX, MPE/iX, and HP Secure OS Software for Linux). You will continue to receive all security bulletin digests unless you choose to update your subscriptions.

To update your subscriptions, use your browser to access the IT Resource Center on the World Wide Web at:

<http://www.itresourcecenter.hp.com/>

Under the Maintenance and Support Menu, click on the "more..." link. Then use the 'login' link at the left side of the screen to login using your IT Resource Center User ID and Password.

Under the notifications section (near the bottom of the page), select Support Information Digests.

To subscribe or unsubscribe to a specific security bulletin digest, select or unselect the checkbox beside it. Then click the "Update Subscriptions" button at the bottom of the page.

o IT Resource Center World Wide Web Service

If you subscribed through the IT Resource Center and would like to be REMOVED from this mailing list, access the IT Resource Center on the World Wide Web at:

<http://www.itresourcecenter.hp.com/>

Login using your IT Resource Center User ID and Password. Then select Support Information Digests (located under Maintenance and Support). You may then unsubscribe from the appropriate digest.

Digest Name: daily HP-UX security bulletins digest
Created: Tue Feb 26 8:45:03 PST 2002

Table of Contents:

Document ID Title

HPSBUX0202-184 Sec. Vulnerability in SNMP (rev. 3)

The documents are listed below.

Document ID: HPSBUX0202-184

Date Loaded: 20020212

Title: Sec. Vulnerability in SNMP (rev. 3)

TEXT

****REVISED 03** HEWLETT-PACKARD COMPANY SECURITY BULLETIN: #0184,**

Originally issued: 12 Feb. 2002

Last revised: 24 Feb. 2002

The information in the following Security Bulletin should be acted upon as soon as possible. Hewlett-Packard Company will not be liable for any consequences to any customer resulting from customer's failure to fully implement instructions in this Security Bulletin as soon as possible.

PROBLEM: Vulnerabilities in SNMP request and trap handling.

PLATFORM: HP 9000 Series 700 and Series 800 running HP-UX releases 10.X and 11.X

HP Procurve switches

****REVISED 03****

---->> JetDirect Firmware

MC/ServiceGuard, EMS HA Monitors

DAMAGE: Possible denial-of-service, service interruptions, unauthorized access.

SOLUTION: Apply patches or implement workarounds. See below.

For HP-UX releases:

PHSS_26137 s700_800 HP-UX 10.20 OV EMANATE14.2 Agent

PHSS_26138 s700_800 HP-UX 11.X OV EMANATE14.2 Agent

PSOV_03087 Solaris 2.X EMANATE Release 14.2

For systems running OV NNM:

PHSS_26286 s700_800 HP-UX 10.20 ovtrapd large trap fix

PHSS_26287 s700_800 HP-UX 11.X ovtrapd large trap fix

PSOV_03100 Solaris 2.X ovtrapd large trap fix

NNM_00857 NT 4.X/Windows 2000 ovtrapd large trap fix

MANUAL ACTIONS: Upgrade or workaround action per below.

AVAILABILITY: Patches for some affected systems are available now.

CHANGE SUMMARY: Rev.01 affected HP Procurve scope expanded,
plus Procurve patch availability added.

NNM ovtrapd patch availability added.

Rev.02 SG and EMS found not vulnerable.

Rev.03 Jetdirect vulnerability updated

A. Background

CERT has issued an advisory:

CERT Advisory CA-2002-03 Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol (SNMPv1) containing information about the vulnerabilities.

Hewlett-Packard Company will revise this bulletin as new information becomes available.

hp Procurve switches

We are still in the process of determining which other HP Procurve products are subject to these vulnerabilities. We have created fixes for products below which will resolve these issues. See Section C below.

Customers can download these patches in the form of software upgrades at:

<http://www.hp.com/rnd/software/switches.htm>

Product Fix revision number

- HP Procurve Switch 2524 (J4813A) F.04.08 or greater
- HP Procurve Switch 2512 (J4812A) F.04.08 or greater
- HP Procurve Switch 4108GL (J4865A) G.04.05 or greater
- HP Procurve Switch 4108GL-bundle (J4861A) G.04.05 or greater

Not all HP Procurve products have completed testing, nor are they listed here, and may or may not have these vulnerabilities. This bulletin will again be updated as new information becomes available.

 NNM (Network Node Manager)

Some problems found in NNM product were related to trap handling. Patches are available. See Section C below.

****REVISED 03****

 -->> JetDirect Firmware

JetDirect Firmware Version State

- =====
- >> X.08.32 and lower VULNERABLE
 - >> (where X = A through K)
 - >> X.21.00 and higher NOT vulnerable
 - >> (where X = L through P)

 HP-UX Systems running snmpd or OPENVIEW

Any HP-UX 10.X or 11.X system running snmpd or snmpdm is vulnerable. To determine if your HP-UX system has snmpd or snmpdm installed:

```
swlist -l file | grep snmpd
```

B. Fixing the problem

Install the appropriate patch or firmware revision or work around problem as detailed below.

C. Recommended solution

hp Procurve switches

Customers can download these patches in the form of software upgrades at:

<http://www.hp.com/rnd/software/switches.htm>

Product Fix revision number

HP Procurve Switch 2524 (J4813A) F.04.08 or greater

HP Procurve Switch 2512 (J4812A) F.04.08 or greater

HP Procurve Switch 4108GL (J4865A) G.04.05 or greater

HP Procurve Switch 4108GL-bundle (J4861A) G.04.05 or greater

NNM (Network Node Manager)

Problems found in the NNM product (related only to trap handling) are addressed in patches available at:

http://support.openview.hp.com/cpe/patches/nnm/6.2/s700_800_11.X.jsp

PHSS_26286 s700_800 HP-UX 10.20 ovtrapd large trap fix

PHSS_26287 s700_800 HP-UX 11.X ovtrapd large trap fix

PSOV_03100 Solaris 2.X ovtrapd large trap fix

NNM_00857 NT 4.X/Windows 2000 ovtrapd large trap fix

MC/ServiceGuard

MC/ServiceGuard is not affected. Testing has been completed and neither MC/ServiceGuard nor ServiceGuard OPS Edition are negatively impacted.

The ServiceGuard Manager product does not use the cluster SNMP and remains unaffected.

Event Monitoring System (EMS)

Testing of the MC/ServiceGuard or ServiceGuard OPS Edition application with package resources defined using EMS High Availability Monitors has been completed and shows no vulnerability to this issue.

****REVISED 03****

--->> JetDirect Firmware

JetDirect Firmware Version State

=====

--->> X.08.32 and lower VULNERABLE

--->> (where X = A through K)

--->> X.21.00 and higher NOT vulnerable

--->> (where X = L through P)

--->>FIX STATUS: HP is working on a firmware fix.

--->>WORKAROUND: Change the set-community-name and use the

--->>Access Control List as described in "HP Jetdirect Print

--->>Servers - Making HP Jetdirect Print Servers Secure on

--->>the Network":

--->> http://www.hp.com/cposupport/networking/support_doc/

--->> bpj05999.html#P88_10129

--->> LIMITING THE VULNERABILITY

--->>SNMPv1 security relies on the set community name. It is

--->>important that a set-community-name be configured on the

--->>Jetdirect device and that it be kept secret.

--->>Jetdirect Print Servers offer an Access Control List that

--->>can be used to specify which hosts can make SNMP

--->>configuration changes to Jetdirect Print Servers.

--->>The steps above can help prevent exploitation of the

--->>vulnerability. To eliminate the vulnerability before a fix

--->>is available SNMP can be disabled on the Jetdirect device.

--->> DISABLING SNMP ON A JETDIRECT PRINT SERVER

--->>1. Update the firmware to the highest level as described in

--->> the Jetdirect Upgrade Instructions document:

--->> http://www.hp.com/cposupport/networking/support_doc/bpj06917.html

--->>NOTE: Disabling SNMP may affect device discovery and port monitors that use SNMP to get status on the device.
--->> Use this feature with care.

--->>2. Telnet to the Jetdirect device (on the latest firmware)
--->> and type:
--->> snmp-config: 0
--->> quit

--->>This will completely disable SNMP on the Jetdirect device.

--->>HP always recommends upgrading Jetdirect firmware for the latest bug fixes and security benefits. The upgrade firmware and download utility are available free of charge:

--->>http://www.hp.com/cposupport/networking/support_doc/bpj06917.html

--->>The following is a list of JetDirect Product Numbers that can be freely upgraded to X.08.32 or X.21.00 or higher firmware. The latest firmware revision available for download is given. For example, the latest firmware revision for the J3110A is G.08.32.

--->>EIO (Peripherals Laserjet 4000, 5000, 8000, etc...)

--->> J3110A 10T [G.08.32]
--->> J3111A 10T/10B2/LocalTalk [G.08.32]
--->> J3112A Token Ring (discontinued) [G.08.32]
--->> J3113A 10/100 (discontinued) [G.08.32]
--->> J4169A 10/100 [L.21.22]
--->> J4167A Token Ring [L.21.25]
--->> J6057A 10/100 [R.22.09]

--->>MIO (Peripherals LaserJet 4, 4si, 5si, etc...)

--->> J2550A/B 10T (discontinued) [A.08.32]
--->> J2552A/B 10T/10Base2/LocalTalk (discontinued) [A.08.32]
--->> J2555A/B Token Ring (discontinued) [A.08.32]
--->> J4100A 10/100 [K.08.32]

- >> J4105A Token Ring [K.08.32]
- >> J4106A 10T [K.08.32]

- >> LIO (Peripherals Color Inkjet cp1160, cp1700)
- >> J6042A 250m 10/100 [N.21.22]

- >> External Print Servers
- >> J2591A EX+ (discontinued) [E.08.32]
- >> J2593A EX+3 10T/10B2 (discontinued) [D.08.32]
- >> J2594A EX+3 Token Ring (discontinued) [D.08.32]
- >> J3263A 300X 10/100 [H.08.32]
- >> J3264A 500X Token Ring [J.08.32]
- >> J3265A 500X 10/100 [J.08.32]
- >> J6038A 310x USB 10/100 [Q.22.04]

HP-UX Systems running snmpd or OPENVIEW

The following patches are available now:

- PHSS_26137 s700_800 HP-UX 10.20 OV EMANATE14.2 Agent\$
- PHSS_26138 s700_800 HP-UX 11.X OV EMANATE14.2 Agent\$
- PSOV_03087 Solaris 2.X EMANATE Release 14.2 \$

All three patches are available from:

<http://support.openview.hp.com/cpe/patches/>

In addition PHSS_26137 and PHSS_26138 are now available from:

<http://itrc.hp.com>

=====
NOTE: The patches are labeled OV (Open View). However, the patches are also applicable to systems that are NOT running Open View.
=====

Workaround for HP-UX Systems:

If a patch is not available for your platform or you cannot install an available patch, snmpd and snmpdm can be disabled by removing their entries from /etc/services and removing the execute permissions from /usr/sbin/snmpd and /usr/sbin/snmpdm.

D. To subscribe to automatically receive future NEW HP Security Bulletins from the HP IT Resource Center via electronic mail, do the following:

Use your browser to get to the HP IT Resource Center page at:

<http://itrc.hp.com>

Use the 'Login' tab at the left side of the screen to login using your ID and password. Use your existing login or the "Register" button at the left to create a login, in order to gain access to many areas of the ITRC. Remember to save the User ID assigned to you, and your password.

In the left most frame select "Maintenance and Support".

Under the "Notifications" section (near the bottom of the page), select "Support Information Digests".

To -subscribe- to future HP Security Bulletins or other Technical Digests, click the check box (in the left column) for the appropriate digest and then click the "Update Subscriptions" button at the bottom of the page.

or

To -review- bulletins already released, select the link (in the middle column) for the appropriate digest.

To -gain access- to the Security Patch Matrix, select the link for "The Security Bulletins Archive". (near the bottom of the page) Once in the archive the third link is to the current Security Patch Matrix. Updated daily, this matrix categorizes security patches by platform/OS release, and by bulletin topic. Security Patch Check completely automates the process of reviewing the patch matrix for 11.XX systems.

For information on the Security Patch Check tool, see:

http://www.software.hp.com/cgi-bin/swdepot_parser.cgi/cgi/displayProductInfo.pl?productNumber=B6834AA

The security patch matrix is also available via anonymous ftp:

ftp://itrc.hp.com/~ftp/export/patches/hp-ux_patch_matrix

On the "Support Information Digest Main" page: click on the "HP Security Bulletin Archive".

E. To report new security vulnerabilities, send email to

security-alert@hp.com

Please encrypt any exploit information using the security-alert PGP key, available from your local key server, or by sending a message with a -subject- (not body) of 'get key' (no quotes) to security-alert@hp.com.

Permission is granted for copying and circulating this Bulletin to Hewlett-Packard (HP) customers (or the Internet community) for the purpose of alerting them to problems, if and only if, the Bulletin is not edited or changed in any way, is attributed to HP, and provided such reproduction and/or distribution is performed for non-commercial purposes.

Any other use of this information is prohibited. HP is not liable for any misuse of this information by any third party.

-----End of Document ID:
HPSBUX0202-184-----

Re: Hewlett Packard HP3000 - MPE vulnerable to CERT® Advisory CA-2002-03 SNMP

This is resolved on HP-e3000 MPE/iX systems - fix:
8606-248966 in the following patches to the SNMP Agent:

SNMGDL9 for C.60.00
SNMGDM0 for C.65.00
SNMGDM1 for C.70.00

Hirschmann Electronics GmbH & Co. KG

Hirschmann Electronics GmbH & Co. KG supplies a broad range of networking products, some of which are affected by the SNMP vulnerabilities identified by CERT Coordination Center. The manner in which they are affected and the actions required to avoid being impacted by exploitation of these vulnerabilities, vary from product to product. Hirschmann customers may contact our Competence Center (phone +49-7127-14-1538, email: ans-support@nt.hirschmann.de) for additional information, especially regarding availability of latest firmware releases addressing the SNMP vulnerabilities.

Hitachi Data Systems (HDS)

Hitachi Data Systems (HDS) has evaluated the information about the industry wide SNMP (Simple Network Management Protocol) vulnerabilities and is conducting the appropriate series of

tests to determine the possible exposure on its entire product offering.

While a potential vulnerability has already been assessed in certain product's configurations, HDS has designed the necessary temporary workaround and made them available to our customers through the local support personnel. As soon as a permanent fix will become available, it will be immediately provided to all our customers.

For further details please contact the Hitachi Data System technical support structure or visit our web site at:

http://www.hds.com/products_services/support/

IBM Corporation

The AIX operating system is susceptible to the vulnerabilities tested for by the Oulu University PROTOS test suite for all levels of AIX 4.3.x prior to level 4.3.3.51, and AIX 5.1 prior to level 5.1.0.10. APARs were developed and made available last year that closed the vulnerabilities looked for by the test suite. For 4.3.x, the relevant APAR is #IY17630; for 5.1, the appropriate APAR is #IY20943.

To see if your version and level of AIX is vulnerable, enter the command:

```
lspp -l bos.net.tcp.client
```

If the "Level" stated is lower than those given above, your system is vulnerable, and you are urged to apply the appropriate APAR.

AIX versions prior to 4.3 are also vulnerable, but these versions are no longer supported by IBM.

To remain consistent with IBM's standing agreement with our customers who use zOS and OS/400, IBM asks that these customers contact IBM Service for information regarding this vulnerability.

InfoVista

In reference to CERT Advisory CA-2002-03, Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol (SNMP), InfoVista has reviewed and addressed this advisory that reports how vulnerabilities may allow unauthorized privileged access, denial of service attacks, or unstable behavior.

InfoVista has assessed the InfoVista product portfolio and investigated the impact of this advisory. Tests have been performed against the PROTOS c06-snmv1 test suite and as a result, InfoVista products fixes are being created, if needed, which will resolve any related issues. Upgrades to our product line that address these issues will be released in the near future.

A status of each InfoVista product is as follows:

InfoVista Server

The InfoVista Server is not affected by trap & agent-side vulnerabilities. The InfoVista Server performs numerous consistency checks on SNMP packets, thus being immune to most attacks. Further evaluation is underway to assess any vulnerability and, if exposures as reported in the advisory are found, fixes will be provided.

Vista Plug-in for NetFlow

The Vista Plug-in for NetFlow version 3.0 includes Emanate 15.2.1.7, which does not address these vulnerabilities. The latest version of Emanate 15.3.1.7, which accounts for these vulnerabilities, will be included in the next version of the Vista Plug-in for NetFlow. A product release schedule will be communicated soon.

Vista Plug-in Family

Full testing of our agents for the vulnerabilities identified in CERT Advisory CA-2002-03, VU#854306 and VU#107186 have been completed. A hotfix for the Vista Plug-in Family that corrects these vulnerabilities is scheduled for release at the end of March.

VistaNotifier

VistaNotifier is not affected by agent-side vulnerabilities. VistaNotifier does consistency checks for traps, while expecting these traps to be in a specific format (from the InfoVista server), thus being immune to most attacks. Further evaluation is underway to assess any vulnerability and, if exposures as reported in the advisory are found, fixes will be provided.

Inktomi Corporation

All releases of Inktomi Traffic Server and Inktomi Media-IKT prior to version 5.2 are vulnerable, releases after 5.2 are not vulnerable. A software patch is available to close the vulnerability.

Download and installation instructions are available at:

ftp://traffic_swul:nc0ming@support.inktomi.com/CA-2002-03/README

Traffic Server deployed as part of the Inktomi Content Networking Platform 1.0 is also vulnerable, and should be immediately updated to v1.1 or 1.1.1. Inktomi CNP customers can get the 1.1.1 release from <http://downloads.inktomi.com>.

Other Inktomi Products:

Inktomi CDS is not vulnerable. CDS is safe because it does not listen for SNMP requests. Inktomi

Enterprise Search is also not vulnerable, because it does not include any SNMP. Finally, Inktomi Media Distribution Network is also safe because it does not include any SNMP.

Innerdive Solutions, LLC

Innerdive Solutions, LLC has two SNMP based products:

1. The "SNMP MIB Scout" (<http://www.innerdive.com/products/mibscout/>)
2. The "Router IP Console" (<http://www.innerdive.com/products/ric/>)

The "SNMP MIB Scout" is not vulnerable to either bug.

The "Router IP Console" releases prior to 3.3.0.407 are vulnerable. The release of "Router IP Console" correcting the behavior outlined in OUSPG#0100 is 3.3.0.407 and is already available on our site. Also, we will notify all our customers about this new release no later than March 5, 2002.

INRANGE Technologies

The CERT Coordination Center has issued a broad based alert to the technology industry, including INRANGE Technologies, regarding potential security vulnerabilities identified in the Simple Network Management Protocol (SNMP), a common networking standard. The company is assessing the issue with its products. Updates will be posted to the INRANGE website (<http://www.inrange.com>) as circumstances dictate.

InterNiche Technologies, Inc.

InterNiche Technologies, Inc.'s SNMPv1 product is not susceptible to problems described in CERT Advisory VU#107186, and the company is in the process of evaluating the behavior of its implementation with respect to Advisory VU#854306.

It is unclear at this point whether the product is vulnerable to attack as described in this second advisory (VU#854306), and if any problems are discovered InterNiche customers will be notified and a fix made available under the terms of their support agreement.

iPlanet

Update on CERT ALERT CA-2002-03

iPlanet has identified a problem in the CERT Alert CA-2002-03, regarding implementations of its directory server and web proxy server.

The SNMP agent (magt) daemon supplied with the Admin Server component of Netscape Directory Server 4.1x, iPlanet Directory Server 5.0, iPlanet Directory Server 5.1 and iPlanet Web Proxy Server 3.6 on UNIX platforms is vulnerable to a malformed request. The malformed request will cause the "magt" daemon to abruptly exit, so that it will no longer accept requests. The "magt" daemon is not included in the Admin Server component of the Netscape Directory Server or iPlanet Directory Server on the Windows NT, Windows 2000 platforms and is not used on AIX

platforms, so the Directory Server and Web Proxy Server are not affected on these platforms.

This vulnerability is present in the following versions running on Unix platforms:

Netscape Directory Server 4.12, 4.13, 4.14, 4.15 and 4.16

iPlanet Directory Server 5.0, 5.0SP1 and 5.1

iPlanet Web Proxy Server 3.6

We do not believe that this vulnerability affects the overall integrity of the directory server or web proxy server in any way.

As a general practice, we recommend disabling all services affected by the "magt" daemon that are not explicitly required until a patch is downloaded and installed. If you are not using SNMP to monitor the directory server, we recommend that you do not run the "magt" daemon process. You can also limit your exposure to this vulnerability by using a firewall to restrict access to the UDP port on which "magt" receives incoming SNMP requests.

Patches and Service packs fixing this problem will be posted under <http://www.iplanet.com/downloads/patches/>.

Version Recommended action

Directory Server 4.1x Install standalone "magt" patch

Directory Server 5.0 Upgrade to 5.0SP2 or install "magt" patch

Directory Server 5.0SP1 Upgrade to 5.0SP2 or install "magt" patch

Directory Server 5.1 Install standalone "magt" patch

iPlanet Web Proxy Server 3.6 Install standalone "magt" patch

iPlanet products, such as iPlanet Application Server Enterprise Edition 6.x, bundling the above mentioned products are also affected. Installing the appropriate Directory Server patches and/or service pack is recommended.

iPlanet customers with questions on this advisory are requested to contact iPlanet Technical Support who will provide full support and up-to-date information.

Ipswitch, Inc.

Ipswitch has completed its assessment of WhatsUp Gold in response to the CERT advisory (CA-2002-03). We have addressed all of the issues highlighted by the CERT advisory's 24,000 test cases via a patch release.

A free patch is currently available to upgrade WhatsUp Gold customers from version 7.01 to 7.02. You can download the patch from <http://www.ipswitch.com/support/whatsup/patch-upgrades.html>.

For customers who are currently running WhatsUp Gold version 6.02, a patch will be released

shortly to upgrade you to version 6.03. Please check back with our patch page (<http://www.ipswitch.com/support/whatsup/patch-upgrades.html>) over the next couple of weeks.

Thank you for your continued support of WhatsUp Gold and other Ipswitch products.

iTouch Communications

iTouch Communications has confirmed that the following tests failed (software crash) in the MX and InReach Series run-time image Xpcsrv20.sys version 6.3 and NEMC_IR.SYS version 3.0 and earlier:

1. APP tests, 10545 and 10549
2. ENC tests 878,7643,7686,7687,7688,13358 & 13486

These issues were fixed in Xpcsrv20.sys version 6.3s15 and NEMC_IR.SYS version 3.0s1 and now they are fully compliant with the SNMP vulnerability CERT tests.

Customers requesting software updates or more information may contact iTouch Communications at 800-435-7997 (domestic) and 978-952-4888 (International) and select the Customer Service option.

Juniper Networks

This is in reference to your notification regarding CAN-2002-0012 and CAN-2002-0013. Juniper Networks has reproduced this behavior and coded a software fix. The fix will be included in all releases of JUNOS Internet software built after January 5, 2002. Customers with current support contracts can download new software with the fix from Juniper's web site at <http://www.juniper.net>

Note: The behavior described in CAN-2002-0012 and CAN-2002-0013 can only be reproduced in JUNOS Internet software if "snmp traceoptions flag pdu" is enabled. Tracing of SNMP PDUs is generally not enabled in production routers.

KarINet, Inc.

Karlnet Advisory:
SNMPv1 Implementation Vulnerabilities in Karlnet Products
Revision 1.0
Revision Date: 14 March 2002

I Vulnerabilities Found

Preliminary test results have indicated multiple Karlnet products exhibit certain vulnerabilities to SNMP messages. Some of these vulnerabilities can be exploited, resulting in a denial of service or service interruption.

These results have not indicated any vulnerability that will allow an attacker to gain access to the

affected device.

II. Solution

In response to CERT® Advisory CA-2002-03 Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol (SNMP), Karlnet Inc. has detected and repaired all of the inconsistencies found by CERT Tests in our SNMP implementation. We have ensured that all vulnerabilities found, using test suite, PROTOS c-06-SNMPv1, have been corrected and implemented in all versions of Karlnet Software 4.01 or greater.

Kentrox,LLC

Kentrox, LLC.. has reviewed CERT Advisory CA-2002-03 and has published the results of our initial evaluation. Kentrox will continue testing products that support SNMP against the PROTOS test suite. As results become available they will be added to the information found at our web site.

The results can be found at: <http://www.kentrox.com/cert-CA-2002-03-response>.

Lantronix, Inc.

Lantronix is committed to resolving security issues with our products. The SNMP security bug you reported has been fixed in LRS firmware version B1.3/611(020123).

Larscom Incorporated

Larscom Incorporated has completed a preliminary examination of its product line in response to CA-2002-03. Larscom has identified a number of platforms that use SNMP, both V1 and V2. It is felt that those using SNMP V2 are not affected by the referenced vulnerabilities.

A complete report listing the affected products and the recommended circumvention can be found at http://www.larscom.com/support/advisory/cert_ca_2002_03.pdf or can be requested from service@larscom.com.

Lexmark International, Inc.

Lexmark International has tested the current MarkNet network adapters and current Lexmark Utilities (MarkVision Professional) according to recommendations issued by CERT. Lexmark Utilities are not vulnerable. Below is a list of tested MarkNet devices and information on obtaining updated network firmware when necessary:

Printer/Network Adapter type	Fix Revision (if applicable)
Lexmark E322n Laser Printer	4.20.14 or greater
Lexmark T520n Laser Printer	Not vulnerable
Lexmark T522n Laser Printer	Not vulnerable
Lexmark T620n Laser Printer	Not vulnerable
Lexmark T622n Laser Printer	Not vulnerable

Lexmark Optra W810n Laser Printer	3.20.14 or greater
Lexmark W820n Laser Printer	Not vulnerable
Lexmark Optra C710nSBE Laser Printer	3.20.14 or greater
Lexmark Optra C710n Laser Printer	3.20.14 or greater
Lexmark C720n Color Laser Printer	3.20.14 or greater
Lexmark C720dn Color Laser Printer	3.20.14 or greater
Lexmark C750n Color Printer	Not vulnerable
Lexmark C750dn Color Printer	Not vulnerable
Lexmark C910n Color Printer	Not vulnerable
Lexmark C910dn Color Printer	Not vulnerable
Lexmark Optra Color 45n	3.20.14 or greater
Lexmark Optra T610n Laser Printer	3.20.14 or greater
MarkNet N2001e	3.20.14 or greater
MarkNet N2000t	3.20.14 or greater
MarkNet N2002e	3.20.14 or greater
MarkNet N2003fx-MTRJ	3.20.14 or greater
MarkNet N2003fx-SC	3.20.14 or greater
MarkNet N2401e	5.20.14 or greater
MarkNet N2501e	5.20.14 or greater
MarkNet X2011e	4.20.14 or greater
MarkNet X2012e	4.20.14 or greater
MarkNet X2030t	4.20.14 or greater
MarkNet X2031e	4.20.14 or greater
MarkNet XI	4.20.14 or greater
MarkNet XP	4.20.14 or greater
MarkNet Pro network family	2.10.193 or greater
MarkNet S network family	1.10.193 or greater
Lexmark X820e MFP	Not vulnerable
Lexmark X7500 MFP	Not vulnerable

None of the Lexmark network adapters are vulnerable once the community name is changed. If unable to update to one of the above firmware levels, Lexmark recommends changing the community name.

Firmware updates are available at: http://support.lexmark.com/en/cert_ca-2002-03.html

For questions related to these or other Lexmark devices please contact 1-800-LEXMARK.

Lotus Development Corporation

Lotus Software evaluated the Lotus Domino Server for vulnerabilities using the test suite materials provided by OUSPG.

This problem does not affect default installations of the Domino Server. However, SNMP agents can be installed from the CD to provide SNMP services for the Domino Server (these are located in the /apps/sysmgmt/agents directory). The optional platform specific master and encapsulator agents included with the Lotus Domino SNMP Agents for HP-UX and Solaris have been found to be vulnerable. For those platforms, customers should upgrade to version R5.0.1 a of the Lotus Domino SNMP Agents, available for download from the Lotus Knowledge Base on the IBM Support Web Site (<http://www.ibm.com/software/lotus/support/>). Please refer to Document #191059, "Lotus Domino SNMP Agents R5.0.1a", also in the Lotus Knowledge Base, for more details.

LOGEC Systems Inc

The products from LOGEC Systems are exposed to SNMP only via HP OpenView. We do not have an implementation of SNMP ourselves. As such, there is nothing in our products that would be an issue with this alert.

Lucent

Lucent is aware of reports that there is a vulnerability in certain implementations of the SNMP (Simple Network Management Protocol) code.

As soon as we were notified by CERT, we began assessing our product portfolio and notifying customers with products that might be affected.

Our 5ESS(R) switch and our optical portfolio were not affected. We have developed, tested, and deployed fixes for most of the impacted products, including our core and edge ATM switches and our edge and broadband access products. Fixes for the rest of the affected product portfolio will be available shortly.

Customers with questions about product vulnerability and/or the status of fixes for affected products should log in to the customer support section of the Lucent web site at <http://www.lucent.com>. Customers who need help registering for the web site should talk to their Lucent customer teams.

Marconi

Marconi supplies a broad range of telecommunications and related products, some of which are affected by the SNMP vulnerabilities identified here. The manner in which they are affected and the actions required (if any) to avoid being impacted by exploitation of these vulnerabilities, vary from product to product. Those Marconi customers with support entitlement may contact the appropriate Technical Assistance Center (TAC) for additional information. Those not under support entitlement may contact their sales representative.

Mercury Interactive Corporation

Of the Mercury Interactive products, both Topaz and SiteScope have the capability to listen to SNMP traps. In both cases this capability is not installed by default. In order to eliminate any vulnerabilities we have taken the necessary steps to verify that our products are immune to the issues mentioned in the advisory.

The SiteScope product version 7.5 and onwards, uses Cyberons for Java from Netaphor Software Inc., with the latest patches. These libraries are immune to the issues mentioned in the advisory. More information about this can be found at <http://www.netaphor.com/Products/CERTAdvisory.html> The Topaz product version 4.1 and onwards, uses the SNMP++ libraries by Agent++, at version 3.1.4b or later. These libraries are immune to the issues mentioned in the advisory. More information about this can be found at http://www.agentpp.com/CERT_SNMPv1_Advisory/body_cert_snmpv1_advisory.html.

Customers using these products, with the capability to listen to SNMP traps, are advised to upgrade to the appropriate version. Mercury Interactive also recommends considering one or more of the following solutions to minimize your network's potential exposure to these vulnerabilities:

- Ingress filtering
- Egress filtering
- Filter SNMP traffic from non-authorized internal hosts
- Change default community strings

Metrobility Optical Systems

Metrobility Optical Systems has identified some of the vulnerability outlined in CERT Advisory CA-2002-03 and is addressing the issue. A technical advisory has been released. Please go to the following web site for information: <http://www.metrobility.com/support/cert.htm>.

MG-SOFT Corporation

MG-SOFT is currently performing detailed verification of the SNMP (SNMPv1, SNMPv2c and SNMPv3) engine implementation.

So far we have noticed that our WinSNMP implementation, the core of all our SNMP products, is vulnerable only in one case. We will post fixed versions of all affected MG-SOFT's SNMP products in few days, on our web site at <http://www.mg-soft.com/>.

Micromuse

Micromuse has published the following response to this advisory:
<http://www.micromuse.com/supportgate/certadvisoryca2002-03.html>

This will be continually updated.

Microsoft Corporation

The following documents regarding this vulnerability are available from Microsoft:
<http://www.microsoft.com/technet/security/bulletin/MS02-006.asp>

ModLink Networks

We ran all recommended tests and found no problems in handling them. All tests passed, no memory leaks, out of bound array references, or crashing were reported.

Monfox, LLC

Monfox has completed testing of our Java DynamicSNMP(TM) Agent and Manager Development Toolkits in accordance with advisory CA-2002-03. Releases of DynamicSNMP prior to Version 3_3_2 are susceptible to 3 of the test cases under certain conditions.

A new release containing fixes for all known vulnerabilities is now available for download. We will provide patch releases for prior versions upon request in the event that any customer is not in the position to upgrade to the latest version.

For more information, please feel free to contact Monfox by email at info@monfox.com or by phone at 678-771-4239.

Multinet

MultiNet and TCPware customers should contact Process Software to check for the availability of patches for this issue. A couple of minor problems were found and fixed, but there is no security risk related to the SNMP code included with either product.

Muonics

Muonics added SNMP management-role (request originator) capabilities to its MIB Smithy series of products starting with version 2.0. Notification (trap/inform) processing was added in version 2.1 (the current version as of this report). Neither version supports agent-role (request processor) capabilities at this time. However, all PDU types are fully parsed by both versions, including requests, before unsupported PDU types are discarded by the dispatcher layer. Both versions of MIB Smithy SDK, from which all of the MIB Smithy series are derived, have been fully tested with all four of the PROTOS c06-SNMPv1 Test Suites. Version 2.0 binds to any available port for sending requests and receiving responses. Since this was not conducive to testing, a special build was required, with the only difference from the official 2.0 release being a hard-coded binding to ports 161 and 162 as appropriate. Version 2.1 allows configuration of a bind port for receiving notifications, so it was not an issue for that version. After running the full series of tests we found both versions to behave as expected, with no signs of failure. We have thus concluded that Muonics' past and current product versions are not susceptible to the security vulnerabilities associated with CA-2002-03.

VU#107186 - Not Vulnerable

VU#854306 - Not Vulnerable

nCipher Corp.

nCipher Corp. supplies two SNMP products:

- 1) a SNMP agent bundled with the nForce/nShield and older nFast products (nFast 75, 150 and 300)
- 2) The SNMP support software bundled with the newer nFast800 products.

The first product (bundled with the nForce, nShield and nFast 75/150/300 range) is a customised NET-SNMP agent version 4.2.1. This is vulnerable to VU#854306 but not VU#107186. nCipher has upgraded this software to the NET-SNMP release 4.2.3 and this is now available as a patch release (see below).

The second product (bundled with the nFast800 product) has two operating modes, one for Linux (and, in the near future, Solaris) and one for Windows NT/2000. In each case, the only agent used is the one currently installed on the OS (NET-SNMP for Linux/Solaris and the Microsoft SNMP agent for Windows); the nCipher-supplied software runs in a separate process.

Customers using this product should therefore ensure that their operating system SNMP agent is patched against this vulnerability.

On Linux or Solaris , this requires installation of the NET-SNMP version 4.2.2 or greater. Running 'snmpd -v' (make sure it is in your path) will tell you the version of the NET-SNMP agent you are currently running.

On Windows, this will require installation of the forthcoming patch from Microsoft. If you have not installed the patch from Microsoft and the 'SNMP Service' is running then you are affected.

Again, if upgrading is not currently possible customers are advised to disable the SNMP service if it might be exposed to hostile network traffic, or make use of other suggestions supplied elsewhere in CERT advisory CA-2002-03.

nCipher has released a specific advisory, which may be obtained from <http://www.ncipher.com/support/advisories/> - this includes a patch to download that upgrades the nCipher agent to version 4.2.3 of the NET-SNMP kit and fixes the issues listed above. Installation instructions are contained within the patch file.

NEC Corporation

updated on March 28, 2002

[Server Products]

* EWS/UP 48 Series

- OS's of all versions are vulnerable.
- SNMP should be off, if not necessary.
- The patches are available through anonymous FTP from:

FTP server: ftp.biglobe.ne.jp

directory: ~ftp/pub/48pub/security/

Please refer to the README file in the directory.

- Detail information in Japanese is at:

< <http://www.mid.comp.nec.co.jp/48info/48patch/ca200203snmpd.html>>

[Software Products]

* Network management system:

+ ESMPRO/ServerManager, ESMPRO Manager

- is vulnerable.

- The patch will be available in the end of March.

- Detail information in Japanese is at:

< <http://www.express.nec.co.jp/care/Security/snmp58.html>>

+ ESMPRO/ClientManager(MG), ESMPRO/ClientManager SmallBusiness Pack

- is vulnerable.

- The patch will be produced.

+ ESMPRO/Netvisor

- is vulnerable.

- The patch will be produced.

+ SystemScope/UXServerManager (Viewer,WindowsMG)

- is vulnerable.

- The patch will be produced.

+ OpenDiosa/OPBASE Base Manager-L (Windows version)

- is vulnerable.

- The patch will be produced.

[Router Products]

* Octpower Series

IP8800/700 Series (710,720,730,735,740,750)

IP8800/600 Series (610,620MM,620SM,620SS,630)

ES8800/1700 Series (1711,1712,1720,1730)

MegaAccessRouter Series (MA25UX/4EMA155MX/4EMA155SX/4E)

MegaAccess Series (MA25LU/4EMA155LM/4EMA155LS/4E)

SH380/200

- are vulnerable.

- The patch is available at:
< <http://www.octpower.nec.co.jp/download/index.html>>
- Detail information in Japanese is at:
< <http://www.octpower.nec.co.jp/news/snmp.html>>

- * CX5200 Series (CX5220,CX5210)
CX4200 Series (CX4220,CX4210)
 - are vulnerable.
 - To get fixed software, please contact to:
<mailto: BQOS@ipnw.jp.nec.com>
 - More information (in Japanese):
< <http://www1.ias.biglobe.ne.jp/IPNW/BQOS/whatsnew.html>>

[VoIP GW/RAS Products]

- * CX3200
 - is vulnerable.
 - To get fixed software, please contact to:
<mailto: BQOS@ipnw.jp.nec.com>
 - More information (in Japanese):
< <http://www1.ias.biglobe.ne.jp/IPNW/BQOS/whatsnew.html>>

[Other Network Equipment Products]

[Devices and other products]

net.com

Network Equipment Technologies, dba net.com
Security Advisory:
SNMPv1 Request and Trap Handling Vulnerabilities
Release Date: 22 February 2002

On February 12, 2002 the CERT®/CC released an advisory related to security vulnerabilities that may exist in network devices using SNMPv1 as the management protocol. In response to this advisory, CERT® Advisory CA-2002-03 Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol (SNMP)", net.com began executing the tests that elicit these vulnerabilities for all net.com products that feature SNMPv1 capability.

Preliminary analysis indicates that multiple net.com products may exhibit certain vulnerabilities to SNMP messages as described in this Advisory. net.com is currently applying the PROTOS

c06-SNMPv1 test suite to all products that feature SNMPv1 capability. Until net.com has completed testing on all of its products and provided patches or fixes to eliminate these vulnerabilities, net.com recommends one or more of the following best practices, as identified in CERT® Advisory CA-2002-03, to minimize your network's potential exposure to these vulnerabilities:

- Disable SNMP on workstations or devices not being managed by SNMP managers.
- Ingress filtering
- Egress filtering
- Filter SNMP traffic from non-authorized internal hosts
- Segregate SNMP traffic onto a separate management network
- Restrict SNMP traffic to Virtual Private Networks (VPNs)
- Change default community strings

For more information please see: www.net.com/service/

NetSilicon

The PROTOS c-06-SNMPv1 test suite provides evidence that the NetSilicon Softworks SNMP v1/v2/v3 agent Release 2 is not susceptible to the vulnerabilities described in this alert. Existing customers, with support agreements, using Release 1 of the agent can receive a free upgrade to Release 2 via the customer support link of the NetSilicon Softworks web site at <http://www.netsilicon.com/Sftwrks/Support/helpdesk.asp>.

NET-SNMP

All ucd-snmp version prior to 4.2.2 are susceptible to this vulnerability and users of versions prior to version 4.2.2 are encouraged to upgrade their software as soon as possible (<http://www.net-snmp.org/download/>). Version 4.2.2 and higher are not susceptible.

Netaphor

NETAPHOR SOFTWARE INC. is the creator of Cyberons for Java -- SNMP Manager Toolkit and Cyberons for Java -- NMS Application Toolkit, two Java based products that may be affected by the SNMP vulnerabilities identified here. The manner in which they are affected and the actions required (if any) to avoid being impacted by exploitation of these vulnerabilities, may be obtained by contacting Netaphor via email at info@netaphor.com Customers with annual support may contact support@netaphor.com directly. Those not under support entitlement may contact Netaphor sales: sales@netaphor.com or (949) 470 7955 in USA.

NetBSD

NetBSD does not ship with any SNMP tools in our 'base' releases. We do provide optional packages which provide various support for SNMP. These packages are not installed by default, nor are they currently provided as an install option by the operating system installation tools. A system administrator/end-user has to manually install this with our package management tools. These SNMP packages include:

- netsaint-plugin-snmp-1.2.8.4 (SNMP monitoring plug-in for netsaint)

- p5-Net-SNMP-3.60 (perl5 module for SNMP queries)
- p5-SNMP-3.1.0 (Perl5 module for interfacing to the UCD SNMP library)
- p5-SNMP_Session-0.83 (perl5 module providing rudimentary access to remote SNMP agents)
- ucd-snmp-4.2.1 (Extensible SNMP implementation) (conflicts with ucd-snmp-4.1.2)
- ucd-snmp-4.1.2 (Extensible SNMP implementation) (conflicts with ucd-snmp-4.2.1)

We do provide a software monitoring mechanism called 'audit-packages', which allows us to highlight if a package with a range of versions has a potential vulnerability, and recommends that the end-user upgrade the packages in question.

Netscape Communications Corporation

Netscape continues to be committed to maintaining a high level of quality in our software and service offerings. Part of this commitment includes prompt response to security issues discovered by organizations such as the CERT® Coordination Center.

According to a recent CERT/CC advisory, The Oulu University Secure Programming Group (OUSPG) has reported numerous vulnerabilities in multiple vendor SNMPv1 implementations. These vulnerabilities may allow unauthorized privileged access, denial of service attacks, or unstable behavior.

We have carefully examined the reported findings, performing the tests suggested by the OUSPG to determine whether Netscape server products were subject to these vulnerabilities. It was determined that several products fell into this category. As a result, we have created fixes which will resolve the issues, and these fixes will appear in future releases of our product line. To Netscape's knowledge, there are no known instances of these vulnerabilities being exploited and no customers have been affected to date.

When such security warnings are issued, Netscape has committed to - and will continue to commit to - resolving these issues in a prompt and timely fashion, ensuring that our customers receive products of the highest quality and security.

NetScout Systems, Inc.

NetScout has determined that some of its products were affected by the warning issued by the CERT Coordination Center of vulnerabilities in the processing of Simple Network Management Protocol (SNMP) messages. As a result, we have implemented patches, that protect our customers from a potential attack..

NetScout customers can obtain necessary patches by going to the Software Download area on our Web site at www.netscout.com/support. The patches are found in a directory named "SNMP Security Patch." Please contact Customer Support if you require assistance.

It is important to note that the NetScout probes are passive devices and as such pose no risk to the network if compromised by an attack exploiting these vulnerabilities.

In an effort to help our customers minimize the risk of this vulnerability to other SNMP enabled devices, NetScout has provided instructions on how our products can be used to help defend against attacks. These instructions are available on our Web site at <http://www.netscout.com/support/alert.htm>.

If you have further questions regarding the SNMP vulnerabilities warning, please contact Customer Support at 1-888-357-7667, or 1-978-614-4370 for assistance.

NetScreen

NetScreen's Global PRO and Global PRO Express do not have an SNMP agent or manager and are not sensitive to the issues raised in VU#107186 (CAN-2002-0012), "Multiple vulnerabilities in SNMP v1 trap handling". No change in behavior or operation is required.

NetScreen determined that the SNMP agent within all versions of ScreenOS is sensitive to certain of the issues described in VU#854306 (CAN-2002-0013), "Multiple vulnerabilities in SNMP v1 request handling". These vulnerabilities can in certain circumstances be exploited to produce a denial of service. These vulnerabilities cannot be used to gain management control of the device.

NetScreen has developed and tested maintenance releases of ScreenOS software that address these vulnerabilities. All NetScreen security appliances and systems shipped from NetScreen after Wednesday 13 February 2002 have software pre-installed at the factory that addresses these vulnerabilities. Customers may download maintenance releases from the NetScreen support web site (<http://www.netscreen.com/support/>).

Network Appliance

Information about the vulnerability of our systems has been posted on our primary support site: NOW (<http://now.netapp.com>). The following field alert has also been issued to our customers: Field Alert # 120: CERT Advisory CA-2002-03: SNMP Vulnerabilities

Testing shows some NetApp products will be affected by some of the issues listed in the CERT Advisory. Please note that NetCache appliances are only vulnerable if the attack comes from a trusted host.

The following appliances will PANIC when under attack: F85, F87, F820, F840, F880, C1100 series, C3100, C6100. The following appliances were not observed to panic, but they may still be vulnerable to attack: F720, F740, F760, C720, C760. Information about the bug associated with this vulnerability can be found in Bugs Online area of NOW (<http://now.netapp.com>).

What happens when a filer/cache is hit by these cases?

The NetApp system will PANIC with a PANIC string similar to the following:

PANIC: Protection Fault accessing address 0x00000001 from EIP 0x5f02c9 in process snmpd on release NetApp Release Rxxxxxxx on Wed Feb 13 02:19:14 2002

What releases have the fix for this issue?

Patches have been built for the following OS levels:

Data ONTAP 5.3.7R3 - Patch is 5.3.7R3D12

Data ONTAP 6.1.1R2 - Patch is 6.1.1R2D16

Data ONTAP 6.1.2R1 - Patch is 6.1.2R1D4

NetCache 5.1 - Patch is 5.1R2D22

NetCache 5.2.1 - Patch is 5.2.1R1D2

The patches for both Data ONTAP and NetCache are available on the NOW site.

What will I see if someone attempts to attack my machine and I have installed an OS with the fix?

You will see a message similar to the following in the messages log and the filer or NetCache will continue to function normally.

```
Wed Feb 13 21:57:56 GMT [snmpd:warning]: SNMP detected possible buffer overflow attempt, skipping request
```

For more information visit <http://now.netapp.com>

Network Associates

PGP is not affected, impacted, or otherwise related to this VU#.

Network Computing Technologies

Network Computing Technologies has reviewed the information regarding SNMP vulnerabilities and is currently investigating the impact to our products.

NETWORK HARMONi, Inc.

Network Harmoni's response to CERT Advisory CA-2002-03

The CERT/CC is part of the Networked Systems Survivability (NSS) Program at the Software Engineering Institute (SEI), Carnegie Mellon University. The primary goal of the NSS Program is to ensure that appropriate technology and systems management practices are used to resist attacks on networked systems and to limit damage and ensure continuity of critical services in spite of successful attacks. On February 12th, 2002, CERT issued two advisories that warn of problems that could arise as the result of improper handling of malformed packets by applications using

SNMP protocols. The Oulu University Secure Programming Group (OUSPG) had discovered that improperly formed packets in the form of trap messages to SMNP managers and request messages to SNMP agents had caused problems in a number of SNMP based products. A list of vendors, with products based on SNMP, was compiled by CERT, and they were notified directly along with the press and analyst community covering the Network Management space.

Once we were notified of the situation, we immediately began regression testing our agent software against the entire Protos Test Suite: c06-snmpv1 used by Oulu University to discover these two packet handling vulnerabilities. Because we are not currently offering products that accept trap messages, testing was focused on the ability of our SNMP agents to handle malformed SNMP requests without incident. It was discovered through our testing that both RMONplus and SLAplus are potentially vulnerable to this method of disruption and will exhibit unpredictable behavior as a result of running this test suite. Rather than issue a patch, we have made modification to both versions of our agent to correct this problem. Customers concerned about vulnerabilities related to CERT Advisory CA-2002-03 should contact NETWORK HARMONi at support@networkharmoni.com for a new build.

Current status (Wednesday 2/20/2002 4:00 PM):

RMONplus & SLAplus (Builds 232 and above)

Sun Solaris - Passed All tests

Windows XP - Passed All tests

Windows 2000 - Passed All tests

Windows NT - Passed All tests

HP-UX - Passed All tests

IBM AIX - Passed All tests

Linux - Passed All tests

Nokia

This vulnerability is known to affect IPSO versions 3.1.3, 3.3, 3.3.1, 3.4, and 3.4.1. Patches are currently available for versions 3.3, 3.3.1, 3.4 and 3.4.1 for download from the Nokia website. In addition, version 3.4.2 shipped with the patch incorporated, and the necessary fix will be included in all future releases of IPSO.

We recommend customers install the patch immediately or follow the recommended precautions below to avoid any potential exploit.

If you are not using SNMP services, including Traps, simply disable the SNMP daemon to completely eliminate the potential vulnerability.

If you are using only SNMP Traps and running Check Point FireWall-1, create a firewall policy to

disallow incoming SNMP messages on all appropriate interfaces. Traps will continue to work normally.

Nortel Networks

Nortel Networks is cooperating to the fullest extent with the CERT Coordination Center and customers that potentially could be affected and other companies within the networking industry to assess, address, and resolve the situation.

For specific information on Nortel Networks response to CERT Bulletin CA-2002-03, please visit our web site <http://www.nortelnetworks.com/corporate/technology/snmpv1.html>

Novell

Novell ships SNMP.NLM and SNMPLOG.NLM with NetWare 4.x, NetWare 5.x and 6.0 systems. The SNMP and SNMPLOG vulnerabilities detected on NetWare are fixed and available for download. The TID (Technical Information Document) number is 2961546, it can be obtained from the url <http://support.novell.com/servlet/tidfinder/2961546>.

NuDesign Team, Inc.

NuDesign Team, Inc. is a vendor of SNMP Management and Agent software solutions. We have tested our products and identified vulnerabilities identified by VU#854306, VU#107186, and OUSPG#0100 advisories with our SNMP Agent and SNMP Trap receiving products. We have applied required corrections, new versions of NuDesign products have completed the regression test cycle and have been made available to our customers on Feb 18, 2002.

For additional information please contact NuDesign Team, Inc. at 416 737 0328 or visit www.NuDesignTeam.com.

OpenBSD

OpenBSD does not ship SNMP code.

Openwave Systems Inc.

Openwave Systems Inc. acknowledges the potential of SNMP vulnerabilities described in [VU#107186 and VU#854306]. Openwave embeds SNMP in their messaging products for the purpose of internal measuring and monitoring of the messaging system. The vulnerabilities listed above can cause denial of service of the SNMP service when specific malformed packets are delivered, but since most customers do not allow SNMP traffic through their firewall, and only utilize SNMP inside their firewall for the purpose of internal monitoring, they should be immune to the SNMP vulnerabilities listed above. Even if SNMP traffic is allowed through the firewall, or no firewall is employed, the SNMP vulnerabilities above can at most cause denial of service of the SNMP services and cannot cause either unprivileged access or denial of service of the messaging products themselves.

A patch will be made available by Openwave to address the SNMP vulnerabilities. Customers can determine if a patch is needed by inspecting their version of snmpdm via the following command:

```
% ./snmpdm -d
```

Versions which are 15.3.1.7 or greater have no vulnerability. Customers who require upgrades to their version of snmpdm should contact their Openwave Technical Support representative for availability of a patch on their specific product line.

Some customers additionally use a toolkit delivered by Openwave called the "TACPAC". This toolkit contains a utility called snmpttrapd which is also vulnerable to the SNMP issues mentioned above. Customers who use this tool are encouraged to contact their Openwave Technical Support representative to obtain a new version of the tool which removes the vulnerabilities.

Optical Access

Following the release of vulnerability notes VU#107186 and VU#854306, our company OpticalAccess has two product lines of switches and routers with SNMP agent implementations: OptiSwitch and OptiSwitch Master.

Optical Access tested the SNMP agents of our OptiSwitch product line with the original Oulu university test patterns and found them not vulnerable.

The OptiSwitch Master product line uses UCD-SNMP version that was found to be vulnerable. UCD-SNMP version that includes the patch for the reported vulnerabilities will be integrated into the next major release. Until then, The use of ACL for management sessions feature can significantly reduce the risk (without compromising performance).

Oracle Corporation

Oracle Security Alert #30

Dated: 5 March, 2002

SNMP Vulnerability in Oracle Enterprise Manager, Master_Peer Agent

Description

A potential security vulnerability has been discovered in the Oracle Enterprise Manager (EM) SNMP monitoring capability for Oracle Database that may result in a potential Denial of Service (DoS) attack against EM's "master_peer" agent.

EM is comprised primarily of two driver programs, the "Intelligent Agent" that performs core EM functionality and the "master_peer" agent that provides monitoring capability for EM when SNMP is being used.

This potential security vulnerability can manifest only when the SNMP monitoring feature is used in addition to the default functionality provided by EM. The "master_peer" agent of EM, which provides the SNMP monitoring capability, is vulnerable to ill-formed SNMP requests that render it unable to respond to further SNMP requests or send unsolicited SNMP messages.

Note: The "Intelligent Agent" is not affected by this potential security vulnerability. Therefore, EM's core functionality such as job submission, event registration, notifications, etc. is not affected.

Products affected

EM Releases 1.6.5, 2.0, 2.1, 2.2, 9.0.1 running on (or "included with"):

- Oracle7 Database, Release 7.3.x
- Oracle8 Database, Releases 8.0.x
- Oracle8i Database, Releases 8.1.x
- Oracle9i Database, Release 9.0.1.x

Platforms affected

Windows and all Unix platforms that support SNMP variants except for IBM AIX.

Workarounds

There are no workarounds to protect against the SNMP vulnerability.

Patch Information

Oracle has fixed the potential vulnerability identified above in patch/bug fix number 2224724. Patches will be available only for supported releases of EM and Oracle Database on all platforms that require a patch.

Download currently available patches for your platform from Oracle's Worldwide Support web site, Metalink, <http://metalink.oracle.com>. Activate the "Patches" button to get to the patches Web page. Enter the patch/bug fix number indicated above and activate the "Submit" button.

Please check Metalink and/or with Oracle Worldwide Support periodically for patch availability if the patch for your platform is not yet available.

Oracle strongly recommends that you comprehensively test the stability of your system upon application of any patch prior to deleting any of the original file(s) that are replaced by the patch.

Credits

Oracle Corporation thanks CERT of Carnegie Mellon University's Software Engineering Institute for bringing this potential security vulnerability to Oracle's attention.

OutBack Resource Group, Inc.

OutBack Resource Group, Inc.

OutBack Resource Group, Inc. acknowledges the potential of SNMP vulnerabilities as identified in the following CERT advisories:

VU#854306 - Multiple vulnerabilities in SNMPv1 request handling

VU#107186 - Multiple vulnerabilities in SNMPv1 trap handling

OutBack has investigated how these vulnerabilities may impact OutBack's jSNMP Enterprise product and has determined the following:

VU#854306 - This advisory is not applicable to jSNMP, because jSNMP does not accept or process SNMP Get, Set, or GetNext PDUs; rather, jSNMP sends those requests to SNMP agents and processes subsequent responses.

VU#107186 - jSNMP v3.2 passed the 24,098 applicable tests in the PROTOS c06-snmpv1 test suite. jSNMP v3.1 failed only one test with undesirable behavior. No consequences, other than potential denial-of-service, are known. There have been no reported instances of this vulnerability being exploited in the jSNMP product.

We recommend that our customers upgrade to the latest available version of jSNMP.

Up-to-date information is available at www.outbackinc.com or support@outbackinc.com.

Paradyne

A recent alert issued by CERT states that any device connected to the Internet has potential security vulnerability. The specific root cause relates to SNMP v1, which is implemented in many Paradyne products. This alert has caused a number of Paradyne customers to call and request an official statement and risk assessment associated with Paradyne's equipment.

The purpose of this document is to inform you that Paradyne engineering staff is currently assessing the situation to determine if any vulnerabilities exist. The analysis will take into consideration product features, SNMP v1 issues and the typical usage of our products in DSL and Frame

Relay network topologies. In typical configurations, direct connection to the Internet with Paradyne devices and/or management systems is extremely rare.

Please note that while no device is completely secure, Paradyne has implemented several safeguards that protect against intrusion such as that identified by CERT Advisory CA-2002-03. Prior to the time that Paradyne releases a more comprehensive statement, we recommend that you take the following actions as appropriate:

- Change community string from public; choose obscure names
- Use device SNMP access list capability
- Use firewall at NOC if NOC has access to Internet, same for CEU central site products (FrameSaver)
- Utilize inband management (dedicated management PVC) when possible

Taken together, these methods provide a robust security feature set which should minimize the impact of the concerns raised in the CERT alert. With this said, Paradyne will release a more complete assessment as soon as possible. This response will consist of an analysis of the overall security risks, recommendations to mitigate these risks and, if necessary, plans for the introduction of new code to close any identified security breaches.

Perle Systems

With regard to CERT Advisory CA-2002-03, it has been recognized by Perle Systems that specific Perle products may be exposed to these SNMP vulnerabilities. Perle is addressing these vulnerabilities across all affected product lines and has released an advisory and solution guide at: http://www.perle.com/support_services/index.shtml

Powerware Corporation

Powerware Corporation notice regarding CERT SNMP Vulnerability Announcement and popular Powerware Connectivity Devices

Most customers operate firewalls that block externally originating SNMP traffic, and further, detect and prevent Denial of Service attacks. It is these devices that constitute a main focal point of SNMP concern since they represent the vanguard of your network.

Based upon SNMP blocking and ingress/egress filtering, any possible potential security vulnerability may only be exploited by users who have access to your local security domain, therefore the risk is diminished.

Testing has revealed the following:

Powerware, to date, knows of no SNMP-related security issues with its legacy, internal and external, ConnectUPS SNMP cards. Testing with the ConnectUPS and BestLink SNMP/Web Card has revealed that the card can, under direct attack, cease to respond to further network requests. This resulting behavior does not affect the operation of the underlying UPS. A firmware patch will be available on the Powerware web site shortly (www.powerware.com).

Qualcomm

WorldMail does not support SNMP by default, so customers who run unmodified installations are not vulnerable.

Quallaby Corporation

QUALLABY's findings to date regarding the recent CERT advisory are as follows:

CERT Advisory CA-2002-03

VU#854306 - Multiple Vulnerabilities in SNMPv1 Request Handling -

This advisory is not applicable to PROVISIO as it is a management system and not an agent. As a management system, PROVISIO does not accept SNMP requests. PROVISIO sends SNMP requests and processes subsequent SNMP responses.

CERT Advisory CA-2002-03

VU#107186 - Multiple Vulnerabilities in SNMPv1 Trap Handling -

This advisory is not applicable to PROVISIO as it does not accept SNMP Trap PDU. PROVISIO only sends SNMP Traps.

Quick Eagle Networks

Quick Eagle Networks, Inc. is a provider of intelligent WAN access solutions for IP and frame relay networks, and the world leader in multilink access devices. Quick Eagle Networks continues to be committed to ensure a high level of security and reliability of our customer's networks. Part of this commitment includes prompt responses to security issues discovered by organizations such as the CERT® Coordination Center.

I. Overview

On February 12, 2002 the CERT®/CC released an advisory related to security vulnerabilities that may exist in network devices using SNMPv1 as the management protocol. In response to this advisory (CERT Advisory CA-2002-03: Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol), Quick Eagle Networks Inc. began immediately investigating whether these vulnerabilities impact Quick Eagle's products.

II. Test Procedures

Quick Eagle Networks is currently applying the PROTOS c06-SNMPv1 test suite to all products and its variations that feature SNMPv1 capability. The tests evaluate the robustness of the application logic of the SNMPv1 implementation as well as the robustness of the BER decoder of the SNMPv1 implementation.

III. Impact

Preliminary test results have not indicated any vulnerability that will allow an attacker to gain access. In general, Quick Eagle Networks' products use out of band management, eliminating the chances of an attacker to gain access from the outside of a network. While most of Quick Eagle Networks' newer WAN access devices have already passed the test, some of Quick Eagle Networks' older products are still under investigation.

IV. Solution

Until Quick Eagle Networks has completed testing on all of its products and provided patches or fixes to eliminate these vulnerabilities, Quick Eagle Networks recommends considering one or more of the following solutions, as also identified in CERT® Advisory CA-2002-03, to minimize your network's potential exposure to these vulnerabilities:

- Disable SNMP on the device
- Change the default community strings
- Disconnect the management port. This won't have any impact on your network traffic as Quick Eagle's solutions use out of band management.

The recommendations above apply only for those products that are still under evaluation. Please refer to our status report for further information.

IV. Status Reports

For more information please visit <http://www.quickeagle.com/support/cert.asp>

RAD Data Communications Ltd.

The security of our customer's networks is of highest priority to RAD Data Communications Ltd. ("RAD"). RAD is aware of CERT's Advisories VU#854306 and VU#107186, and is working together with its partners to assess if any of its products might be affected.

VU#107186: RAD's Network Management System (RADview) is not vulnerable to the extent of working in conjunction with 3rd party products, such as Castle Rock's SNMPc 5, HP's NNM 6.2, Microsoft's Windows NT4 and Sun's Solaris 2.7. Customers are advised to consult the respective

responses of these vendors, available at <http://www.kb.cert.org/vuls/id/854306> and verify that they comply with each vendor's specific recommendations.

VU#854306: As a first measure, we have requested from 3rd party software developers, the products of which are integrated within RAD's SNMP agents and Network Management station, to provide us with statements as to their products vulnerabilities and their potential impact. We are currently waiting for their conclusions. In parallel, RAD is in process of internally setting up the testing schedules and facilities to ascertain the vulnerability of our products.

Radware

Radware has assessed its SNMP based products against the vulnerabilities identified in CERT Advisory CA-2002-03. The following table identifies by product the currently available software maintenance releases that include the fix for the SNMP vulnerabilities:

<i>Product</i>	<i>Release (HW Platforms)</i>
WSD	6.18.02 (H, C)
	7.10.08 (AS2, AS1, H, C)
	7.20.02 (AS1, H)
	7.21.02 (AS2, AS1)
CSD	3.30.02 (AS2, AS1)
	3.40.01 (AS2, AS1)
FP	2.20.09 (AS1, H, C)
LP	3.20.09 (AS1, H, C)
CertainT 1002	2.00 (Model A, Model B)

Radware customers can download this software from the following link:

<http://www.radware.com/content/support/customers/downloads/index.htm>

Radware Channel Partners can download this software from the following link:

<http://www.radware.com/content/support/techresources/prodinfo/SWStatusMatrix.htm>

For upgrades within the same feature release, e.g. WSD 7.10.07 to WSD 7.10.08, software passwords are not needed.

For upgrades to a new feature release, e.g. WSD 7.10.07 to WSD 7.21.02, a software password is needed and can be obtained by contacting Radware technical support at support@radware.com.

The unit must be covered by an active support agreement to obtain a password for a feature release upgrade. Additional requirements, e.g. minimum Boot ROM software version, may exist.

Software upgrade instructions can be found at the following link:

<http://www.radware.com/archive/support/general/info/upgrades.PDF>

Anyone who does not have access to the restricted areas of the Radware web site or has any other questions regarding these maintenance releases and the upgrade process, can contact Radware Technical Support at support@radware.com for assistance.

At all times, Radware recommends taking the following standard security precautions:

- Disable all remote management access through all unnecessary interfaces using the SNMP or Management Ports Table feature, depending on the specific software release in use.
- If possible, limit all remote management access to a physically separate port that is connected to a secure management segment.

Redback Networks, Inc.

Redback Networks, Inc. has identified that the vulnerability described in CA-2002-03 may affect its products. To that end Redback has been providing security workarounds to protect existing installations and will issue software patches to provide a conclusive solution to the problem. The SmartEdge Transport product line is unaffected by this vulnerability. Customers should contact Redback Networks Technical Assistance Center [Domestic TAC number (877) 733 2225; International TAC number is 31-104987777; Web: www.redback.com/support] for more information and workarounds.

Red Hat

RedHat has released a security advisory at <http://www.redhat.com/support/errata/RHSA-2001-163.html> with updated versions of the ucd-snmp package for all supported releases and architectures. For more information or to download the update please visit this page.

Riverstone Networks

The Riverstone product line is, under certain circumstances, vulnerable to some of the SNMP issues described in CERT's VU#854306 (advisory CA-2002-03). Based on current testing the assessment is that the risk to an operational network is low. Patch releases 7.0.2.6 and 8.0.3.3 will correct these vulnerabilities.

Please implement the following workarounds until these patches are made available:

- create access control lists to allow only trusted management stations to access the router.
- create an exclusive management VLAN to manage the router.
- manage the router through its ethernet management interface.
- or
- disable SNMP

SecureWorks, Inc.

SecureWorks is not vulnerable to SNMP based attacks. The SecureWorks iSensor and Secure Operations Center uses a proprietary protocol in order to remotely monitor and configure devices. Additionally, the SecureWorks iSensor is capable of filtering malformed and/or illegal snmp packets in order to protect against incoming and outgoing SNMP based attacks.

Sierra Wireless

We are not vulnerable.

Sinetica Corporation Limited

<http://www.kb.cert.org/vuls/id/IAFY-56DKEV>

SGI

SGI acknowledges the SNMP vulnerabilities reported by CERT and is currently investigating. No further information is available at this time.

For the protection of all our customers, SGI does not disclose, discuss or confirm vulnerabilities until a full investigation has occurred and any necessary patch(es) or release streams are available for all vulnerable and supported IRIX operating systems. Until SGI has more definitive information to provide, customers are encouraged to assume all security vulnerabilities as exploitable and take appropriate steps according to local site security policies and requirements. As further information becomes available, additional advisories will be issued via the normal SGI security information distribution methods including the wiretap mailing list on <http://www.sgi.com/support/security/>.

Sniffer Technologies

SNMP Request and Trap Handling Security Advisory

Revision 1.0

Release Date: 03/01/02

Sniffer Technologies has prepared this advisory regarding SNMP in Sniffer Technologies products. This advisory contains specific instructions on how to disable these services where security may be an issue.

An update regarding this issue will be sent to all Sniffer Technologies customers on Wednesday, March 13, 2002. The Sniffer Technologies team is working diligently to fully resolve this issue. If you have further questions in the interim, please contact technical support.

What is the SNMP security risk?

On February 12, 2002, The CERT Coordination Center issued a warning that a broad array of network equipment used on the Internet -- including switches, routers, hubs, printers and operating systems -- may be vulnerable to an SNMP-related attack that could cause equipment to fail or allow an attacker to take control of it. Though not mentioned on their list of vendors, our Sniffer Distributed product is another such device that may have this inherent SNMP vulnerability because of its RMON/SNMP capabilities.

There are two areas in our product that can be affected by this security concern.

1. The RMON/SNMP features of our Sniffer Distributed Appliance
2. The Trap Capture application at our SniffView Console

In both cases, these SNMP commands can be disabled on our product if not in use.

Can I avoid using these features in the Sniffer Distributed Product without affecting the capabilities of the Sniffer Product?

Yes, you can disable the SNMP/RMON capabilities of the product and utilize our proprietary method of logging network statistics and Expert Symptom and Diagnosis to disk for reporting with Reporter and/or Sniffer Watch. This method does not utilize SNMP and therefore is not susceptible to the SNMP vulnerability. You will still have the same statistics and reports that are available using the SNMP/RMON features of the product, with the addition of the Expert Symptoms and Diagnosis which are unique to our method of logging and reporting.

How do I turn off these SNMP capabilities in the product?

Turning off SNMP at the Sniffer Distributed Appliance:

By default, the SNMP and RMON features of the Sniffer Distributed Appliance are enabled. To turn off these features, follow the procedures below.

1. Either Start Probe Viewer at the Sniffer Distributed Appliance, or "Configure" an Agent from your SniffView Console.
2. Select the SNMP tab.
3. Disable SNMP Trap
4. Disable SNMP/RMON.
5. Restart the Sniffer Distributed Appliance for changes to take effect.

Turning off the SNMP Trap Capture at the SniffView Console:

By default, when you install the SniffView Console a program called Trap Capture automatically gets installed and runs in the background. This program can accept SNMP Traps from Sniffer Distributed Appliances as well as other SNMP devices. Follow the procedures below to turn it off:

1. Start the SniffView Alarm Manager.
2. Select Toggle Trap capture. The Trap capture program will be disabled. However, if you reboot the PC the SniffView Console is running on it will turn itself back on. Therefore you must remember to disable it again.

Will these features be disabled in the future?

Yes, the SNMP/RMON features of the product will be disabled by default starting with the Sniffer Distributed v4.1 (with Support for Web Console) version.

What if I require these features?

If you require these features then there are a few steps that you can take to protect yourself from this security concern.

1. Under the SNMP Tab (see above) Change Community name from "public" to something else.
2. Using routers and/or firewalls, control SNMP access to the Sniffer Distributed Appliances or SniffView Console to ensure the traffic originates from known management systems and addresses.
3. Filter SNMP services at your network perimeter (ingress/egress filtering).
4. Segregate network management traffic onto a separate network. (i.e. a VPN) Refer to CERT advisory CA-2002-03 (<http://www.cert.org/advisories/CA-2002-03.html>) for more details and the most recent information regarding recommended solutions.

How will this security concern affect my network?

This issue has the potential to create a denial of service attack. An attacker sending bogus SNMP requests and traps could flood the Sniffer Distributed Appliance and/or SniffView console running the Trap Capture application. This might cause the system to hang and may require a reboot.

An attacker should not be able to configure or take control of either the Sniffer Distributed Appliance or the SniffView Console.

Has anyone reported an exploitation of this vulnerability on a Sniffer Distributed system?

No.

Have we notified CERT of our concern?

Yes

Where can I find out more information regarding this security concern?

For more information regarding this vulnerability please refer to the following URLs on CERT's web site:

<http://www.cert.org/advisories/CA-2002-03.html>

http://www.cert.org/tech_tips/snmp_faq.html

SNMP Research International

The most recent releases (15.3.1.7 and above) of all SNMP Research products address the vulnerabilities identified in the following CERT vulnerability advisories:

VU#854306 (Multiple vulnerabilities in SNMPv1 request handling)

VU#107186 (Multiple vulnerabilities in SNMPv1 trap handling)

A few of the malformed packets sent in these tests result in out of bound array references in allocated memory and minor memory leaks. No consequences, other than potential denial of service on some platforms, are known.

All customers who maintain a support contract have received either the new release or the appropriate patch sets to their 15.3.1.1 and later source code releases addressing these vulnerabilities.

Users maintaining earlier releases should update to the current release if they have not already done so. Up-to-date information is available from support@snmp.com.

SonicWALL, Inc.

SonicWALL has tested its products in response to CERT® Advisory CA-2002-03 "Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol (SNMP)," SonicWALL's has found NO evidence of any SNMP vulnerabilities in any SonicWALL Firewall/VPN appliance or Red Creek 3VPN appliances. No updates are required to maintain the integrity of these products.

SonicWALL acknowledges the potential of SNMP vulnerabilities in its SSL offloader products and is currently working to address any potential security issues. However, exposure to vulnerability is extremely low due to the nature of the typical SSL Offloader network configuration. Because the SSL Offloader is located within a secure network environment, rather than at the network perimeter, the only opportunity for attack would be internal. Customers can eliminate the risk by temporarily disabling the SNMP sub-system.

SolarWinds.Net, Inc.

While the SolarWinds tools are not susceptible to the vulnerabilities listed within this advisory, SolarWinds products can be used to determine if SNMP agents contain known vulnerabilities.

SolarWinds supports the recommendations made by CERT regarding SNMP implementations and has released a Router Security Check tool that can be used to check routers and switches for several known SNMP security flaws.

For more information on using the SolarWinds tools to secure your SNMP implementation please visit:

http://www.solarwinds.net/Tools/Security/Security_SNMP.htm

Sonus Networks

Since the release of CERT Advisory CA-2002-03, Sonus Networks has reviewed its product offering and determined a potential issue may exist within its management offering.

The Sonus PSX6000, SGX2000, and Insight products utilize SNMP Research software in the SONScia package that has been identified by its vendor as possibly vulnerable to the exploit. Sonus product versions 3.2.x, 3.3.x, and 3.4.x all have the affected SONScia package. The issue has been resolved in the upcoming 4.0 versions of the PSX6000, SGX2000, and Insight products and concerned customers are advised to upgrade as the software becomes available.

Sonus PSX6000, SGX2000, and Insight products run on top of Sun Microsystems's Solaris operating environment (versions 2.6 and 2.8). Sun Microsystems has identified these operating environments as vulnerable to the exploit IF they are started or used. Given that Sonus Networks software neither starts nor uses the process in question, `snmpdx`, Sonus products are not vulnerable to

the exploit through this Solaris process.

The Sonus GSX9000 does not use the same third party software as other products from Sonus Networks and at this time we have not found any problems relating to its SNMP operation. Negative testing is a routine portion of GSX9000 SQA and to date has not shown any undesired results. We have recently tested the GSX9000 with OUSPG's PROTOS c06-snmpv1 test suite and those tests passed successfully.

Spider Software

Spider is currently investigating this potential problem and, if applicable, a new version of the SNMP agent will be made available through the standard release process of SpiderTCP.

Spider will notify its customers of any new patches resulting from this investigation through the normal support channel.

Standard Networks, Inc.

Standard Networks offers a "mainframe connectivity" family of products under the "UniGate" brand name. These products contain SNMP agents. After reviewing the recent information regarding SNMP vulnerabilities, performing a source code audit and running a variety of publicly available SNMP exploit suites (including the OUSPG test suite), we believe the UniGate product is not vulnerable to the problems described in VU#854306.

SNMP agent services are enabled by default on UniGate after version 3.6.07. (This version was released in late 1995; anyone with a "Year 2000 Compliant" version runs SNMP services.) It is not currently possible to turn on and shut off SNMP services on a UniGate, but it is possible to change the "inquiry" and "update" strings to unusual values (i.e. "m2H9j3s4") to prevent unauthorized access to the machine. Alternatively, a current version of the UniGate software with SNMP "hardcoded off" (3.99.31) is available from Standard Networks directly for customers who feel they need to have this service disabled immediately. (A future version will allow users to toggle SNMP services on and off.)

Attempts to find or exploit SNMP vulnerabilities on a UniGate platform will often cause the UniGate to log those attempts as "Community Errors" or "Misc Errors" on the "SNMP Statistics" screen and/or as "IP: Fragment Msg too big" errors on the main status screen.

Standard Networks' "OpenIT mainframe connectivity" product will also act as an SNMP agent if SNMP is enabled under Windows NT (rare). OpenIT customers are encouraged to follow "Microsoft Corporation's" latest recommendations regarding Windows NT SNMP issues if they are using this service. It is however possible to immediately disable any active SNMP services on any OpenIT platform by stopping the "SNMP" service from the "Services Control Panel."

No other Standard Networks products (i.e. "EMU Terminal Emulator", "ActiveHEAT Host Access", the "MOVEit" family of secure file transfer products) are affected by this issue.

Customers are encouraged to call Standard Networks immediately (+001 608.227.6100) with any questions or concerns about their specific configuration.

Stonesoft

Stonesoft's StoneGate product does not include an SNMP agent, and is therefore not vulnerable to this. Other Stonesoft's products are still under investigation. As further information becomes available, additional advisories will be available at <http://www.stonesoft.com/support/techcenter/>

Sun Microsystems, Inc.

Sun's SNMP product, Solstice Enterprise Agents (SEA), described here: <http://www.sun.com/solstice/products/ent.agents/>

is affected by VU#854306 but not VU#107186. More specifically the main agent of SEA, snmpdx(1M), is affected on Solaris 2.6, 7, 8. Sun has released Security Bulletin #00215.

Sun Security Bulletins are available from: <http://sunsolve.sun.com/security>.

Sun patches are available from: <http://sunsolve.sun.com/securitypatch>.

Sun products which utilize SNMP are listed in the following SunAlert along with their vulnerability status: <http://sunsolve.Sun.COM/pub-cgi/retrieve.pl?doc=fsalert%2F43704>.

Products listed with a vulnerability status of "Under Investigation" will be updated as soon as more information becomes available.

Symantec Corporation

Symantec verified that the snmptrap.exe on the Intruder Alert (ITA) 3.6 agent, if configured to accept SNMP traps from Symantec NetProwler, is susceptible to a communications Denial of Service when the PROTOS test suite is directed against it. The communicator service will be halted, the halt will be logged and the service requires a restart to reinitiate communications.

This should be a very low risk issue to Symantec ITA customers. The snmptrap.exe module is loaded on an ITA agent machine. Depending on customer configuration if the snmptrap module is loaded on an ITA agent located on the internal network of the company then the collector is only vulnerable to an internal attack as long as the firewall rule set blocks snmptrap communications through the firewall.

The functionality of the snmptrap.exe allows smooth integrated alert management of both NIDS and HIDS from a single administrator console. Halting the communicator module disrupts the integrated communications only. Both the NetProwler and the ITA IDS systems continue to function

normally but will require monitoring from separate consoles until the communicator service is restarted.

Symantec takes any product issue such as this very seriously. We have developed a patch for Symantec ITA 3.6 that addresses this problem. The patch is available to Symantec ITA 3.6 customers from the Symantec customer ITA ftp download site as ITA3_6Patch1/061302/. There is a patch for both domestic and international releases.

Please contact [supportolutions@symantec.com](mailto:supportsolutions@symantec.com) for questions on product upgrades.

TANDBERG

Tandberg have run all the testcases found the PROTOS test-suite, c06snmpv1:

1. c06-snmpv1-req-app-pr1.jar
2. c06-snmpv1-req-enc-pr1.jar
3. c06-snmpv1-trap-app-pr1.jar
4. c06-snmpv1-trap-enc-pr1.jar

The tests were run with standard delay time between the requests (100ms), but also with a delay of 1ms. The tests applies to all TANDBERG products (T500, T880, T1000, T2500, T6000 and T8000). The software tested on these products were B4.0 (our latest software) and no problems were found when running the test suite.

Tavve Software Company

Tavve Software Company has investigated its products in light of CERT Advisory CA-2002-03 regarding SNMP vulnerabilities. Tavve's EventWatch, PReView, and Amerigo products always reside within the network management system (NMS) framework supplied by either HP OpenView Network Node Manager or Tivoli NetView; therefore, these Tavve products have no inherent or intrinsic exposure to SNMP vulnerabilities beyond those of the underlying NMS. We advise our customers to apply any patches for Network Node Manger or NetView made available by HP or Tivoli. Tavve has created a solution for ePROBE and will make this update available via its Web site (<http://www.tavve.com>).

Tivoli Systems

Introduction

This document serves as an update regarding the current status of Tivoli/IBM products' implementation of Simple Network Management Protocol (SNMP), Version 1, and the potential vulnerabilities related to the implementation.

Tivoli has identified the following products that implement SNMP v1:

§ Tivoli NetView for Unix

§ Tivoli NetView for Windows

§ Tivoli NetView Mid-Level Manager (MLM)

§ Tivoli Comprehensive Network Address Translator (CNAT)

§ Tivoli NetView for OS/390

§ Tivoli Enterprise Console SNMP Adapter

§ Tivoli Storage Network Manager

§ Tivoli Risk Manager

As an interim step, customers should be directed to secure their networks so as to prevent SNMP access from unknown sources. The CERT advisory contains substantial information on this topic under the heading of “Ingress Filtering”.

The following products have been identified for having the potential exposure:
This information is current as of March 29, 2002.

Identified Loss of Service

The following products have been identified as containing issues that can result in loss of service:

Tivoli NetView for Unix & Windows

DETAILS

Tivoli NetView for Unix & Tivoli NetView for Windows are vulnerable to a loss of service when subjected to certain SNMP get requests or traps as indicated in CA-2002-03.

STATUS

A fix is available (See the section on ‘Fix Locations’).

Tivoli NetView Mid-Level Manager (MLM) Agent for Solaris, HPUX, Windows and AIX

DETAILS

The Tivoli NetView Mid-Level Manager (MLM) on Solaris, HP-UX, Windows and AIX (Version 7.1 and earlier) is vulnerable to a loss of service when subjected to certain SNMP get requests or traps as indicated in CA-2002-03.

STATUS

A fix is currently being tested and will be released. (See the section on 'Fix Locations').

Tivoli Comprehensive Network Address Translator (CNAT)

DETAILS

This product is vulnerable to a temporary loss of service of the AIX system, which causes a loss of connectivity to the portion of the network relying on the CNAT system for NAT routing.

STATUS

A fix is currently being tested and will be released. The fix will be available on this site (See the section on 'Fix Locations').

Tivoli NetView for OS/390 Version 1.2, 1.3, and 1.4

DETAILS:

ABEND in E/AS (Event Automation Services) Trap-to-Alert adapter when Enterprise Object Identification (OID) is very large can occur.

STATUS

A fix is available.

Tivoli Enterprise Console SNMP Adapter

DETAILS

The Tivoli Enterprise Console SNMP Adapter is vulnerable to a loss of service when subjected to certain SNMP get requests or traps.

STATUS

A fix is currently being tested and will be released.

Tivoli Risk Manager

DETAILS

The Tivoli Risk Manager utilizes the Tivoli Enterprise Console SNMP Adapter, which is vulnerable to a loss of service when subjected to certain SNMP get requests or traps as indicated in CA-2002-03.

STATUS

A fix is currently being tested and will be released.

Tivoli Storage Network Manager

DETAILS

This condition only affects TSNM's ability to monitor outband events via SNMP traps. TSNM is capable of managing SANs via both outband mechanisms (SNMP queries to FC switches for topology discovery and receives SNMP traps for outband event detection) and inband mechanisms (managed hosts connected to the SAN via FC HBAs for topology and attribute discovery, and inband FC event detection). Outband discovery, inband discovery, and inband event detection are not affected by this condition.

STATUS

This will be fixed in the next version of TSNM.

PREVENTION

In addition to the prevention noted above, customers should configure at least one Windows or SUN managed host per SAN to allow inband detection of SAN events.

Fix Locations

Service fixes to those products that have identified the issue will post the files in the following 2 locations:

Web - <http://www.tivoli.com/secure/support/documents/security/ca-2002-03.html>

FTP - [ftp.tivoli.com/support/Support_Notes/SecurityBulletins/](ftp://ftp.tivoli.com/support/Support_Notes/SecurityBulletins/)

Questions

For any questions, please contact your local call center or open a PMR through the online support page <http://www.tivoli.com/support/reporting/>.

TMP Consultoria S/C

The Computer Emergency Response Team (CERT) has issued last week an advisory regarding numerous vulnerabilities affecting most vendors' SNMP implementations. This advisory, which can be accessed on <http://www.cert.org/advisories/CA-2002-03.html>, specifically addressed vulnerabilities on the implementations' handling of SNMPv1 trap and request PDUs (more specifically, the handling of the Trap, Get, Set, and GetNext PDUs).

TMP would like to state that we have evaluated the impact of those vulnerabilities on our WANView line of network management solutions, and that we are in NO WAY vulnerable to any of the issues reported, as follows:

VU#854306 - Multiple Vulnerabilities in SNMPv1 Request Handling: This advisory is not applicable to WANView, because WANView does not accept or process in any way SNMP Get/Set/GetNext PDUs; rather, WANView sends those requests to the monitored equipment, and process subsequent responses.

VU#107186 - Multiple Vulnerabilities in SNMPv1 Trap Handling: This advisory is not applicable to WANView either, because WANView currently does not accept SNMP traps (this has been a product design decision) WANView can be configured to send SNMP traps to other systems, and is not affected in this regard.

In case you have any questions or need further assistance regarding these matters, please contact us at <wanview@tmp.com.br>.

Top Layer Networks

Both of Top Layer's focused security appliances, the IDS Balancer and the Attack Mitigator, do not exhibit the SNMP vulnerabilite(s) Outlined by CERT Advisory CA-2002-03.

Neither of these products require any modification at all in order to be protected. The AppSwitch/AppSafe product is also capable of being so protected, but it may require that one configuration change be made to ensure total protection based on the TopPath version of firmware it is running.

The detail of the configuration change required in the AppSwitch/AppSafe product is discussed below.

CERT's recommended restrictions are as follows:

1. Disable SNMP V1 access to all applicable network devices
2. Filter SNMP traffic from non-authorized internal hosts
3. Segregate SNMP traffic onto a separate management network

Top Layer is well positioned to provide immediate solutions for our customers. There are two options that users can immediately choose from to protect their TLN security systems from SNMP V1 attacks:

OPTION 1

All currently shipping Top Layer products come pre-configured from the factory or can be configured to meet CERT restriction # 1. For example, Top Layer's focused security appliances, the IDS Balancer and the upcoming Attack Mitigator products have, as their factory default settings, Access Restrictions for SNMP set to -Denied- thus meeting CERT restriction # 1.

NOTE: The AppSwitch/AppSafe Release 4.1 factory default is for SNMP disabled. Models running Release 3.55 must be explicitly configured to deny access as described above.

OPTION 2

Option #2 is to implement restrictions # 2 and # 3 simultaneously

Restriction # 2

To meet CERT restriction # 2, network managers can set access restrictions for SNMP to an allowed IP host address range via the Web Management Interface supplied with the AppSwitch/AppSafe 3500, the IDS Balancer, and upon general release, the Attack Mitigator. Existing customers can implement this protection themselves in the field today.

Restriction #3

The currently shipping AppSwitch/AppSafe 3500 security device can be configured to restrict SNMP to a single management port via its web management interface. This meets CERT restriction # 3.

Both the IDS Balancer and the Attack Mitigator are designed with separate management ports for that exclusive use. These management ports cannot be accessed via "outside" (public network) or "inside" (internal network) LAN connections for greater security and management system integrity. These products meet CERT restriction # 3 -out of the box-.

BOTTOM LINE

Top Layer's standard offerings meet the criteria that allow users to protect against SNMP V1 vulnerability exploits. This is all part of Top Layer's continued commitment to provide our customers with improved performance and greater security against cyber threats.

Toshiba International Corporation

Toshiba International Corporation
SNMPv1 Request and Trap Handling Vulnerabilities

This is in reference to the CERT Advisory CA 2002-03 regarding security vulnerabilities that may exist in network devices using SNMPv1 such as the TIC SNMP enabled product, RemotEye & RemotEyeII.

Patches are being developed to repair these vulnerabilities. Please visit the RemotEyeII web site at <http://RemotEye.Tic.Toshiba.com> for the expected date for patch availability.

Trend Micro

Trend Micro R&D has determined that Interscan Messaging Services Suite, Scan Mail for Lotus Notes and Scan Mail for Exchange, which all use Simple Network Management Protocol (SNMP) are not affected by SNMP vulnerabilities listed in the CERT® Advisory CA-2002-03 Multiple Vulnerabilities bulletin of February 27.

Unisphere Networks

CUSTOMER SERVICE TECHNICAL BULLETIN

SUBJECT: CERT Advisory CA-2002-03: Vulnerability in SNMP Implementation
BULLETIN NUMBER: ERX_PSN-005
BULLETIN TYPE: Product Support Notification
AFFECTED PRODUCTS: ERX
ISSUE DATE: 03/08/2002
REVISION: 2.0

PROBLEM DESCRIPTION:

The CERT ® Coordination Center released an advisory on February 12, 2002 entitled, "CERT ® Advisory CA-2002-03 Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol (SNMP)". The URL for the full text of the advisory can be found at:

<http://www.cert.org/advisories/CA-2002-03.html>

AFFECTED PRODUCT(S):
ERX 700/705/1400/1440

SOLUTION:

The following releases of software have been found to suffer no negative effects from execution of the PROTONS c06-SNMPv1 test suite authored by OUSPG, as outlined in CERT Advisory CA-2002-03:

- 2-9-1p15-0
- 2-10-1p1-0
- 3-0-6p6-0
- 3-2-3p1-0
- 3-3-2p1-0
- 3-4-0 REL

Subsequent patches (e.g. 3-0-6p7-0 and greater) and maintenance releases (3-4-1) to those listed above have also tested successfully. All future releases will have been tested against PROTONS c06-SNMPv1 as well. Earlier releases of software will experience higher than average SRP CPU utilization resulting in potential SNMP timeouts while the test suite is running, but recover immediately upon test completion. Packet forwarding during the test is not affected. Affected releases include:

- 2-0-0 2-9-1p14-0
- 2-10-0 2-10-1p0-3
- 3-0-0 3-0-6p5-0
- 3-1-0 3-1-0p2-0
- 3-2-0 3-2-3
- 3-3-0 3-3-2

This Product Support Notification is publicly viewable on the Web at:

http://support.unispherenetworks.com/websupport/CERT/erx_psn-005.pdf

If you have any questions concerning this notice, or to obtain the latest patch release, please contact Unisphere Networks Customer Service.

- Inside the U.S. call: (800) 424-2344
- Outside the U.S. call: (978) 589-9000
- Via the Web @ <http://support.unispherenetworks.com>
- Via e-mail @ support@unispherenetworks.com

Uptime Devices, Inc.

Our engineering group downloaded the test suite and ran it against the our products. Our products passed all tests.

Verilink Corporation

Verilink is aware of the CERT/CC advisory related to security vulnerabilities that may exist in network devices using SNMPv1 as the management protocol, issued February 12, 2002. Verilink has implemented measures to assess which products may be affected by this advisory and is working closely with its customers to identify the impact and possible solutions.

VERITAS Software

Is VERITAS SANPoint Control affected by the Simple Network Management Protocol vulnerabilities cited in CERT Advisory CA-2002-03?

TechNote ID: 245634 Last Updated: April 03 2002 01:37 AM GMT

Email this document to a colleague

Caution! The information in this TechNote is based upon certain assumptions, including product, operating system and platform versions. You can review this information in the

TechNote Summary portion of this document.

This document (245634) is provided subject to the disclaimer at the end of this document.

Symptom:

Is VERITAS SANPoint Control affected by the Simple Network Management Protocol vulnerabilities cited in CERT Advisory CA-2002-03?

Solution:

On February 12, the CERT Coordination Center issued a CERT advisory citing vulnerabilities with multiple vendors Simple Network Management Protocol (SNMP) implementations. VERITAS SANPoint Control (SPC) was tested against the CERT SNMPv1 test suite and it was determined that SPC was affected by VU#107186 having to do with SNMPv1 Trap handling. If SPC is installed on a machine outside of a firewall, or inside of a firewall that does not properly block SNMP traffic, it could be open to a denial-of-service attack from the outside.

This problem has been fixed in SPC 2.1.1. For information on how to download the latest release, refer to technote 235218 (link in the Related sections of this TechNote).

If it is not possible to upgrade, but you feel that your SPC hosts

are at risk, then it will be necessary to disable SNMP traps which will affect SPC monitoring and reporting capabilities. Disabling traps will also affect some array monitoring that is done through traps and may slightly delay status notifications if hardware is being monitored through SNMP polls. For more information on SPC monitoring capabilities, refer to the Monitoring and Resolving Problems on the SAN guide in your SPC documentation set. To disable SNMP traps, modify the sal.conf file as shown here:

```
[Exp.SNMPTRAP]
```

```
DisableTrap=1
```

In addition to disabling SNMP traps through the sal.conf file, it is also necessary to disable the VERITAS Trap Processor.

On Windows:

1. Go to Control Panel>Administrative Tools>Services
2. Double-click on VERITAS Trap Service
3. If the Service Status shows "Started", click the stop button.
4. Change the Startup Type to Disabled
5. Click OK

On Solaris:

Modify the /opt/VRTSspcs/vxspcs script as follows to keep the vxtrapd daemon from starting (location of this file may vary depending on the installation directory of the VRTSspcs package):

```
start_trap ()
{
  SAVEDIR=`pwd`
  # cd $BASE_DIR/VRTSspcs/trap/bin
  # ./vxtrapdstart.sh > /dev/null
  cd $SAVEDIR
}
```

For any additional information on CERT Advisory CA-2002-03, go to the following link: <http://www.cert.org/advisories/CA-2002-03.html>

TechNote Summary:

TechNote Title: Is VERITAS SANPoint Control affected by the Simple Network Management Protocol vulnerabilities cited in CERT Advisory CA-2002-03?

TechNote ID: 245634

Last Updated: April 03 2002 01:37 AM GMT

Related Documents: TechNote: 235218 - What is the latest version of VERITAS SANPoint Control?

TechPDF: 242640 - VERITAS SANPoint Control 2.1 - Monitoring and Resolving Problems on the SAN with SANPoint Control 2.1

This information in this TechNote applies to:

Products: SANPoint Control (UNIX Platforms) 1.0, 1.0.1, 2.0, 2.0.1, 2.1, 2.1.1

SANPoint Control for Windows 2000

Subject: SANPoint Control (UNIX Platforms) - Application - Informational

Languages: English

Operating Systems: Windows 2000 Professional 5.00.2195

Windows 2000 Server 5.00.2195, 5.00.2195 SP 1, 5.00.2195 SP 2,

Windows Powered, Windows Powered SP1, Windows Powered SP2

Windows 2000 Advanced Server 5.00.2195, 5.00.2195 SP 1, 5.00.2195

SP 2, Windows Powered, Windows Powered SP1, Windows Powered SP2

Windows 2000 Datacenter Server 5.00.2195, 5.00.2195 SP 1,

5.00.2195 SP 2

Solaris 2.6, 7, 8

Windows NT 4.0 Serv SP4, 4.0 Serv SP5, 4.0 Serv SP6a

VERITAS Software, 1600 Plymouth Street, Mountain View, California

94043 World Wide Web: <http://www.veritas.com>

Tech Support Web: <http://support.veritas.com>

E-Mail for Classic VERITAS Products: support@veritas.com

E-Mail for Classic Seagate Software Products:

helpdesk@support.veritas.com

FTP: <ftp://ftp.support.veritas.com> or <http://ftp.support.veritas.com>

THE INFORMATION PROVIDED IN THE VERITAS SOFTWARE KNOWLEDGE BASE IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. VERITAS SOFTWARE DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL VERITAS SOFTWARE OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER INCLUDING DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES, EVEN IF VERITAS SOFTWARE OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES SO THE FOREGOING LIMITATION MAY NOT APPLY.

Vertical Networks, Inc.

The Vertical Networks InstantOffice product was vulnerable to the SNMP issues VU#854306 and VU#107186. This problem was first corrected in InstantOffice version 4.0 Service Pack 1.

VINA Technologies

Vina is addressing the CERT advisory & evaluating the impact over all its products. Security of our customers networks is of prime importance to us. Integrator 300 & eLink family products have verified no vulnerability with the fix put in place effective 4/08/2002. Testing is still in progress for MX 500/550/600 & MBX 1000 products. Initial results have shown that customers running Frame Relay as WAN protocol are not affected. Action is being taken to evaluate & fix if any PPP or Cisco HDLC encapsulation vulnerabilities are found by running the 'PROTOS c06-snmppv1 test suite' mentioned in the advisory . VINA will continue to update its statement on this site as additional info becomes available.

Westhawk, Ltd.

Westhawk has tested their SNMP stack in Java against the VU#107186 vulnerabilities (Multiple vulnerabilities in SNMPv1 trap handling).

A number of Java exceptions occurred causing possible denial-of-service, but no unauthorized privileged access. These exceptions have been fixed in release 6.0 of our stack and can be found at http://snmp.westhawk.co.uk/snmp6_0.zip?cert.

The stack is capable of receiving request PDUs and sending a response. However it has no support for building the response (it lacks MIB functionality), so running the request test suite for the VU#854306 (Multiple vulnerabilities in SNMPv1 request handling) is currently not applicable.

Wind River Systems, Inc.

Envoy SNMP Agent Source Code v9.0+:

After extensive testing against the PROTOS c06-snmppv1 test suite, we have not been able to reproduce any of the SNMPv1 security problems VU#854306 and VU#107186 in our current

SNMP Source Code products: Envoy SNMP v9.0, v9.1, v9.2, and v9.3 Beta. We ran the tests without seeing any impact on system memory or any other unusual behavior. We encourage all customers to upgrade to the current version of Envoy SNMP Source Code Agent.

WindNet SNMP Agent Binary Objects v2.0:

Testing against the PROTOS c06-snmpv1 test suite has revealed a vulnerability in the current version of WindNet SNMP v2.0. The specific impact is a memory leak caused by the exceptional element E-01. This vulnerability can be demonstrated by test #1421 (among others) in the req-enc test suite. A fix is currently available from Wind River support and on WindSurf for customers with valid maintenance contracts. WindNet SNMP Binary v2.0 customers under maintenance can also eliminate the vulnerability by upgrading to Envoy SNMP Source v9.2. This vulnerability was previously fixed as a "potential leak" in the Envoy v9.0 Agent Source Code release. WindNet SNMP v2.0 is a binary distribution of Envoy v8.0, so it did not include this fix. No current Envoy Source release (v9.0+) is effected by this vulnerability.

Note: As Wind River's Envoy SNMP is a source code product, customer's modifying Envoy MAY introduce vulnerability to VU#854306 and VU#107186. We are especially seeing problems with buffer overruns in customer community string validation routines. Wind River recommends individual testing against the test suite of any customer product incorporating a SNMP agent, particularly MODIFIED Envoy SNMP source code.

Wind River customers under support and maintenance have received the current product releases. Supported customers should Contact Wind River support at support@windriver.com or call (800) 458-7767 with any test reports related to VU#854306 and VU#107186, or for more information. Customers who need to renew support or wish to upgrade to a supported version (Envoy v9.0+ and WindNet SNMP v2.0) should contact their Wind River Account Manager, or 1-800-545-WIND (1-800-545-9463) if they do not have an Account Manager.

World Wide Packets

World Wide Packets

Product notes and recommendations:

LE-2X and 3X portals, LE-2XX and LE-4XX concentrators

Future software releases of WWP Products will address the vulnerabilities identified in the following CERT vulnerability advisories. Current target is to provide patch builds by Q2 '02 that permanently address these issues. Please contact support@wvp.com for details and status.

VU#854306 (Multiple vulnerabilities in SNMPv1 request handling)

VU#107186 (Multiple vulnerabilities in SNMPv1 trap handling)

Until these releases become available, we recommend that the following steps may be taken to help reduce exposure to these vulnerabilities.

In all concentrators:

*Disable SNMP from interfaces through which SNMP commands should not be received, such as those providing connection from the Internet or Extranets.

*Use management VLANs or out-of-band management to contain SNMP traffic and multicasts.

These do not prevent an attacker from exploiting these vulnerabilities, but they may make it more difficult to initiate the attacks.

In the snmp.cfg file of all devices, define the community with the IP address of the Management Station.

Example:

Instead of

```
!snmp_cs_1=1, public, 0.0.0.0, read
```

```
!snmp_cs_2=1, private, 0.0.0.0, write
```

Use

```
!snmp_cs_1=1, <new public string>, <Mgmt Station Ip Address>, read
```

```
!snmp_cs_2=1, <new private string>, <Mgmt Station Ip Address>, write
```

Note: Even when community strings are changed from their defaults, they will still be passed in plaintext and are therefore subject to packet sniffing attacks. SNMPv3 offers additional capabilities to ensure authentication and privacy as described in RFC2574.

LE-3700 Distributor

*Disable SNMP from interfaces through which SNMP commands should not be received, such as those providing connection from the Internet or Extranets

*Use Access Control Lists at the access edge to prevent SNMP traffic from unauthorized internal hosts from entering the network.

*Use management VLANs or out-of-band management to contain SNMP traffic and multicasts.

These do not prevent an attacker from exploiting these vulnerabilities, but they may make it more difficult to initiate the attacks.

*Enable 802.1X port-locking and RADIUS to prevent unauthenticated users from attaching to the network.

Xerox Corporation

Xerox is aware of this advisory. A response regarding all Xerox products that use SNMPv1 is available from our web site: www.xerox.com/security.

Appendix B References

1. <http://www.ee.oulu.fi/research/ouspg/protos/>
2. <http://www.kb.cert.org/vuls/id/854306>
3. <http://www.kb.cert.org/vuls/id/107186>
4. http://www.cert.org/tech_tips/denial_of_service.html
5. <http://www.ietf.org/rfc/rfc1067.txt>
6. <http://www.ietf.org/rfc/rfc1089.txt>
7. <http://www.ietf.org/rfc/rfc1140.txt>
8. <http://www.ietf.org/rfc/rfc1155.txt>

9. <http://www.ietf.org/rfc/rfc1156.txt>
10. <http://www.ietf.org/rfc/rfc1215.txt>
11. <http://www.ietf.org/rfc/rfc1270.txt>
12. <http://www.ietf.org/rfc/rfc1352.txt>

Appendix C Background Information

Background Information on the OUSPG

OUSPG is an academic research group located at Oulu University in Finland. The purpose of this research group is to test software for vulnerabilities.

History has shown that the techniques used by the OUSPG have discovered a large number of previously undetected problems in the products and protocols they have tested. In 2001, the OUSPG produced a comprehensive test suite for evaluating implementations of the Lightweight Directory Access Protocol (LDAP). This test suite was developed with the strategy of abusing the protocol in unsupported and unexpected ways, and it was very effective in uncovering a wide variety of vulnerabilities across several products. This approach can reveal vulnerabilities that would not manifest themselves under normal conditions.

After completing its work on LDAP, OUSPG moved its focus to SNMPv1. As with LDAP, they designed a custom test suite, began testing a selection of products, and found a number of vulnerabilities. Because OUSPG's work on LDAP was similar in procedure to its current work on SNMP, you may wish to review the LDAP Test Suite and CERT Advisory CA-2001-18, which outlined results of application of the test suite.

In order to test the security of protocols like SNMPv1, the PROTOS project presents a server with a wide variety of sample packets containing unexpected values or illegally formatted data. As a member of the PROTOS project consortium, the OUSPG used the PROTOS c06-snmv1 test suite to study several implementations of the SNMPv1 protocol. Results of the test suites run against SNMP indicate that there are many different vulnerabilities on many different implementations of SNMP.

Background Information on the Simple Network Management Protocol

The Simple Network Management Protocol (SNMP) is the most popular protocol in use to manage networked devices. SNMP was designed in the late 80's to facilitate the exchange of management information between networked devices, operating at the application layer of the ISO/OSI model. The SNMP protocol enables network and system administrators to remotely monitor and configure devices on the network (devices such as switches and routers). Software and firmware products designed for networks often make use of the SNMP protocol. SNMP runs on a multitude of devices and operating systems, including, but not limited to,

- Core Network Devices (Routers, Switches, Hubs, Bridges, and Wireless Network Access Points)
- Operating Systems
- Consumer Broadband Network Devices (Cable Modems and DSL Modems)
- Consumer Electronic Devices (Cameras and Image Scanners)
- Networked Office Equipment (Printers, Copiers, and FAX Machines)

- Network and Systems Management/Diagnostic Frameworks (Network Sniffers and Network Analyzers)
- Uninterruptible Power Supplies (UPS)
- Networked Medical Equipment (Imaging Units and Oscilloscopes)
- Manufacturing and Processing Equipment

The SNMP protocol is formally defined in RFC1157. Quoting from that RFC:

Implicit in the SNMP architectural model is a collection of network management stations and network elements. Network management stations execute management applications which monitor and control network elements. Network elements are devices such as hosts, gateways, terminal servers, and the like, which have management agents responsible for performing the network management functions requested by the network management stations. The Simple Network Management Protocol (SNMP) is used to communicate management information between the network management stations and the agents in the network elements.

Additionally, SNMP is discussed in a number of other RFC documents:

- RFC 3000 *Internet Official Protocol Standards*
- RFC 1212 *Concise MIB Definitions*
- RFC 1213 *Management Information Base for Network Management of TCP/IP-based Internets: MIB-II*
- RFC 1215 *A Convention for Defining Traps for use with the SNMP*
- RFC 1270 *SNMP Communications Services*
- RFC 2570 *Introduction to Version 3 of the Internet-standard Network Management Framework*
- RFC 2571 *An Architecture for Describing SNMP Management Frameworks*
- RFC 2572 *Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)*
- RFC 2573 *SNMP Applications*
- RFC 2574 *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*
- RFC 2575 *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)*
- RFC 2576 *Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework*

The CERT Coordination Center thanks the Oulu University Secure Programming Group for reporting these vulnerabilities to us, for providing detailed technical analyses, and for assisting us in preparing this advisory.

We also thank Steven M. Bellovin (AT&T Labs -- Research), Wes Hardaker (Net-SNMP), Steve Moulton (SNMP Research), Tom Reddington (Bell Labs), Mike Duckett (Bell South), Rob Thomas, Blue Boar (Thievco), Sunil Chitnis (Foundry Networks), the Cisco Systems Product Security Incident Response Team (psirt@cisco.com) and the many others who contributed to this document.

Feedback on this document can be directed to the authors, Ian A. Finlay, Shawn V. Hernan, Jason A. Rafail, Chad Dougherty, Allen D. Householder, Marty Lindner, and Art Manion.

This document is available from: <http://www.preview.cert.org/advisories/CA-2002-03.html>

CERT/CC Contact Information

Email: cert@cert.org

Phone: +1 412-268-7090 (24-hour hotline)

Fax: +1 412-268-6989

Postal address:

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
U.S.A.

CERT/CC personnel answer the hotline 08:00-17:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

Using encryption

We strongly urge you to encrypt sensitive information sent by email. Our public PGP key is available from

http://www.cert.org/CERT_PGP.key

If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

CERT publications and other security information are available from our web site

<http://www.cert.org/>

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

NO WARRANTY

Any material furnished by Carnegie Mellon University and the Software Engineering Institute is furnished on an "as is" basis. Carnegie Mellon University makes no warranties of any kind, either expressed or implied as to any matter including, but not limited to, warranty of fitness for a particular purpose or merchantability, exclusivity or results obtained from use of the material. Carnegie Mellon University does not make any warranty of any kind with respect to freedom from patent, trademark, or copyright infringement.

Conditions for use, disclaimers, and sponsorship information

Copyright 2002 Carnegie Mellon University

Revision History

Feb 12, 2002: Initial release
Feb 12, 2002: Corrected vendor appendix formatting issues
Feb 12, 2002: Added vendor statement for Inktomi
Feb 12, 2002: Fixed formatting problem in "Disable stack execution" section
Feb 12, 2002: Updated vendor statement for Juniper
Feb 12, 2002: Fixed broken link in Juniper statement
Feb 12, 2002: Updated Public Thanks section
Feb 12, 2002: Updated Covalent statement
Feb 12, 2002: Updated SNMP Research statement
Feb 12, 2002: Updated CVE and Comtek services links
Feb 13, 2002: Updated vendor statement for Cisco Systems
Feb 13, 2002: Updated vendor statement for Enterasys
Feb 13, 2002: Updated vendor statement for FreeBSD
Feb 13, 2002: Updated vendor statement for HP
Feb 13, 2002: Updated vendor statement for Microsoft
Feb 13, 2002: Updated vendor statement for Sun
Feb 13, 2002: Updated vendor statement for Tandberg
Feb 13, 2002: Removed vendor statement for Tivoli
Feb 14, 2002: Added vendor statement for Aprisma
Feb 14, 2002: Added vendor statements for MG-Soft and NetScreen
Feb 14, 2002: Added vendor statement for iTouch Communications
Feb 14, 2002: Added vendor statement for F5 Networks
Feb 14, 2002: Added vendor statement for Sierra Wireless
Feb 15, 2002: Added vendor statement for MICROMUSE
Feb 15, 2002: Updated HP statement
Feb 16, 2002: Updated Nortel Networks statement
Feb 16, 2002: Added vendor statement for Foundry Networks
Feb 18, 2002: Added vendor statement for Tivoli
Feb 18, 2002: Added vendor statement for Radware
Feb 18, 2002: Updated Nortel Networks statement
Feb 19, 2002: Updated Nortel Networks statement
Feb 19, 2002: Updated F5 Networks statement
Feb 19, 2002: Updated Compaq statement
Feb 19, 2002: Updated IBM statement
Feb 19, 2002: Added vendor statement for Dell
Feb 19, 2002: Fixed bad link in Enterasys statement
Feb 19, 2002: Updated IBM statement
Feb 19, 2002: Added vendor statement for BMC Software

Feb 20, 2002: Added vendor statement for Wind River Systems
Feb 20, 2002: Added vendor statement for Concord Communications
Feb 20, 2002: Added vendor statement for CommWorks Corporation (a 3Com company)
Feb 20, 2002: Added vendor statement for Lexmark International
Feb 20, 2002: Added vendor statement for Check Point Software Technologies Inc.
Feb 20, 2002: Added vendor statement for Alcatel
Feb 21, 2002: Added vendor statement for Avici Systems Inc.
Feb 21, 2002: Added vendor statement for NuDesign Team Inc.
Feb 21, 2002: Added vendor statement for ADTRAN, Inc.
Feb 21, 2002: Updated NetScreen vendor statement
Feb 21, 2002: Added vendor statement for TMP Consultoria S/C
Feb 21, 2002: Added vendor statement for Xerox Corporation
Feb 21, 2002: Updated Inktomi vendor statement
Feb 21, 2002: Added vendor statement for nCipher Corp.
Feb 21, 2002: Updated Lucent vendor statement
Feb 21, 2002: Added vendor statement for Spider Software
Feb 21, 2002: Added vendor statement for Riverstone Networks
Feb 21, 2002: Added vendor statement for Standard Networks, Inc.
Feb 21, 2002: Added vendor statement for Openwave Systems Inc.
Feb 21, 2002: Added vendor statement for General DataComm
Feb 22, 2002: Added vendor statement for NETWORK HARMONi, Inc.
Feb 22, 2002: Updated HP vendor statement
Feb 22, 2002: Updated Nortel Networks statement
Feb 25, 2002: Added vendor statement for American Power Conversion
Feb 25, 2002: Added vendor statement for Cambridge Broadband Ltd.
Feb 25, 2002: Added vendor statement for Corsaire Limited
Feb 25, 2002: Added vendor statement for SonicWALL, Inc.
Feb 26, 2002: Added vendor statement for Perle Systems
Feb 26, 2002: Added vendor statement for Sonus Networks
Feb 26, 2002: Added vendor statement for Optical Access
Feb 26, 2002: Added vendor statement for INRANGE Technologies
Feb 26, 2002: Updated vendor statement for Redback Networks, Inc.
Feb 26, 2002: Removed "Disable stack execution" section from Solutions
Feb 26, 2002: Added vendor statement for BinTec Communications AG
Feb 26, 2002: Updated vendor statement for IBM
Feb 27, 2002: Updated HP vendor statement
Feb 27, 2002: Added vendor statement for World Wide Packets
Feb 27, 2002: Added vendor statement for Dart Communications
Feb 27, 2002: Added vendor statement for Quallaby Corporation
Feb 27, 2002: Updated iTouch Communications vendor statement
Feb 27, 2002: Added vendor statement for CipherTrust, Inc.
Feb 27, 2002: Added vendor statement for Ipswitch, Inc.
Feb 27, 2002: Added vendor statement for D-Link Systems, Inc.

Mar 01, 2002: Added vendor statement for iPlanet
Mar 01, 2002: Updated vendor statement for Novell
Mar 01, 2002: Updated vendor statement for nCipher Corp.
Mar 01, 2002: Added vendor statement for Extreme Networks
Mar 04, 2002: Added vendor statement for NetSilicon
Mar 04, 2002: Added vendor statement for SecureWorks, Inc.
Mar 04, 2002: Added vendor statement for Efficient Networks, Inc.
Mar 04, 2002: Updated vendor statement for Novell
Mar 04, 2002: Added vendor statement for Monfox, LLC
Mar 05, 2002: Added vendor statement for Paradyne
Mar 05, 2002: Added vendor statement for Trend Micro
Mar 05, 2002: Updated vendor statement for Dartware, LLC
Mar 05, 2002: Added vendor statement for Quick Eagle Networks
Mar 05, 2002: Added vendor statement for Conectiva
Mar 05, 2002: Added vendor statement for Asante Technologies, Inc.
Mar 05, 2002: Added vendor statement for SolarWinds.Net, Inc.
Mar 06, 2002: Updated vendor statement for Aprisma
Mar 06, 2002: Updated vendor statement for Ipswitch, Inc.
Mar 06, 2002: Added vendor statement for CSCare, Inc.
Mar 06, 2002: Updated vendor statement for iTouch Communications
Mar 06, 2002: Added vendor statement for Uptime Devices, Inc.
Mar 06, 2002: Added vendor statement for Larscom Incorporated
Mar 06, 2002: Added vendor statement for InterNiche Technologies, Inc.
Mar 07, 2002: Added vendor statement for Network Appliance
Mar 07, 2002: Updated vendor statement for Avaya
Mar 07, 2002: Updated vendor statement for Xerox
Mar 07, 2002: Added vendor statement for Sniffer Technologies
Mar 07, 2002: Added vendor statement for Powerware Corporation
Mar 07, 2002: Added vendor statement for Carrier Access
Mar 07, 2002: Added vendor statement for net.com
Mar 07, 2002: Added vendor statement for Oracle Corporation
Mar 11, 2002: Updated vendor statement for Wind River Systems, Inc.
Mar 12, 2002: Added vendor statement for Apple Computer, Inc.
Mar 12, 2002: Updated vendor statement for Xerox Corporation
Mar 12, 2002: Updated vendor statement for Radware
Mar 13, 2002: Added vendor statement for ADVA AG Optical Networking
Mar 13, 2002: Updated vendor statement for Quick Eagle Networks
Mar 15, 2002: Updated vendor statement for F5 Networks
Mar 18, 2002: Added vendor statement for NEC Corporation
Mar 18, 2002: Added vendor statement for Alvarion Ltd.
Mar 19, 2002: Added vendor statement for e-Security, Inc.
Mar 19, 2002: Updated vendor statement for Concord Communications, Inc.
Mar 19, 2002: Added vendor statement for Equinix Systems
Mar 20, 2002: Added vendor statement for Controlware GmbH

Mar 20, 2002: Fixed broken link in NETWORK HARMONi, Inc. vendor statement

Mar 20, 2002: Updated vendor statement for NETWORK HARMONi, Inc.

Mar 21, 2002: Updated vendor statement for Radware

Mar 21, 2002: Added vendor statement for Unisphere Networks

Mar 21, 2002: Added vendor statement for InfoVista

Mar 21, 2002: Updated vendor statement for COMTEK Services, Inc.

Mar 25, 2002: Added vendor statement for ModLink Networks

Mar 25, 2002: Added vendor statement for Kentrox,LLC

Mar 25, 2002: Added vendor statement for KarlNet, Inc.

Mar 25, 2002: Added vendor statement for Hitachi Data Systems (HDS)

Mar 26, 2002: Added vendor statement for NetScout Systems, Inc.

Mar 26, 2002: Added vendor statement for Verilink Corporation

Mar 26, 2002: Added vendor statement for RAD Data Communications Ltd.

Mar 28, 2002: Updated vendor statement for NEC Corporation

Mar 28, 2002: Added vendor statement for Tavve Software Company

Apr 01, 2002: Updated vendor statement for HP (regarding MPE)

Apr 01, 2002: Added vendor statement for Top Layer Networks

Apr 03, 2002: Updated vendor statement for Tivoli Systems

Apr 04, 2002: Added vendor statement for VERITAS Software

Apr 05, 2002: Added vendor statement for Evidian Inc.

Apr 05, 2002: Added vendor statement for AVET Information and Network Security

Apr 05, 2002: Added vendor statement for Entrada Networks

Apr 05, 2002: Added vendor statement for Cray Inc.

Apr 08, 2002: Added vendor statement for CNT

Apr 09, 2002: Updated vendor statement for Dell

Apr 09, 2002: Updated vendor statement for American Power Conversion

Apr 10, 2002: Updated vendor statement for Dell

Apr 10, 2002: Updated vendor statement for Compaq Computer Corporation

Apr 12, 2002: Added vendor statement for Canoga Perkins Corporation

Apr 16, 2002: Added vendor statement for Toshiba International Corporation

Apr 19, 2002: Added vendor statement for VINA Technologies

Apr 19, 2002: Updated vendor statement for Dell

Apr 22, 2002: Updated vendor statement for Entrada Networks

Apr 24, 2002: Updated vendor statement for VERITAS Software

Apr 24, 2002: Added vendor statement for OutBack Resource Group, Inc.

Apr 26, 2002: Added vendor statement for Fluke Corporation

Apr 28, 2002: Updated vendor statement for DMH Software

May 16, 2002: Updated vendor statement for Sun Microsystems

May 23, 2002: Updated vendor statement for Xerox Corporation

Jun 11, 2002: Updated vendor statement for BMC Software

Jun 11, 2002: Updated vendor statement for BinTec Communications AG
Jun 11, 2002: Updated vendor statement for Symantec Corporation
Jul 25, 2002: Added vendor statement for Digital Networks
Aug 14, 2002: Added vendor statement for Astracon, Inc.
Aug 21, 2002: Updated vendor statement for ADVA AG Optical Network-
ing
Aug 28, 2002: Updated vendor statement for iPlanet
Sep 23, 2002: Added vendor statement for Mercury Interactive Corpo-
ration
Oct 17, 2002: Added vendor statement for Sinetica Corporation Lim-
ited
Nov 05, 2002: Added vendor statement for Future Communications Soft-
ware
May 14, 2003: Added vendor statement for Metrobility Optical Systems
Jun 11, 2003: Added vendor statement for Muonics
Aug 18, 2003: Added vendor statement for Allied Telesyn Interna-
tional
Jul 27, 2004: Updated vendor statement for NuDesign, Inc.
May 24, 2005: Updated vendor statement for Hitachi, removed extra
line before vul note references
November 7, 2007: Closed anchors
February 13, 2008: Added vendor statement for Westhawk

4 CA-2002-04: Buffer Overflow in Microsoft Internet Explorer

Original release date: February 25, 2002

Last revised: April 2, 2002

Source: CERT/CC

A complete revision history can be found at the end of this file.

Systems Affected

Microsoft Windows systems running any of the following:

- Microsoft Internet Explorer
- Microsoft Outlook and Outlook Express
- Other applications that use the Internet Explorer HTML rendering engine

Microsoft Internet Explorer for Macintosh and Internet Explorer for Unix are not vulnerable.

Overview

Microsoft Internet Explorer contains a buffer overflow vulnerability in its handling of embedded objects in HTML documents. This vulnerability could allow an attacker to execute arbitrary code on the victim's system when the victim visits a web page or views an HTML email message.

I. Description

Internet Explorer supports the `<EMBED>` directive, which can be used to include arbitrary objects in HTML documents. Common types of embedded objects include multimedia files, Java applets, and ActiveX controls. The `SRC` attribute specifies the source path and filename of an object. For example, a MIDI sound might be embedded in a web page with the following HTML code:

```
<EMBED TYPE="audio/midi" SRC="/path/sound.mid" AUTOSTART="true">
```

Internet Explorer uses attributes of the `<EMBED>` directive and MIME information from the web server to determine how to handle an embedded object. In most cases, a separate application or plugin is used.

A group of Russian researchers, SECURITY.NNOV, has reported that Internet Explorer does not properly handle the `SRC` attribute of the `<EMBED>` directive. An HTML document, such as a web page or HTML email message, that contains a crafted `SRC` attribute can trigger a buffer overflow, executing code with the privileges of the user viewing the document.

According to the Severity Rating for the "Buffer Overrun in HTML Directive" vulnerability in MS02-005, Internet Explorer 5.5 and 6.0 are vulnerable. Outlook and Outlook Express are also vulnerable, since they use Internet Explorer to render HTML email messages. Other applications

that use the Internet Explorer HTML rendering engine, such as America Online (AOL), Windows compiled HTML help (.chm) files, and third-party email clients may also be vulnerable.

The CERT/CC is tracking this vulnerability as [VU#932283](#), which corresponds directly to the "buffer overrun" vulnerability described in Microsoft Security Bulletin [MS02-005](#). This vulnerability has been assigned the [CVE](#) identifier [CAN-2002-0022](#).

II. Impact

By convincing a user to view a malicious HTML document, an attacker can cause the Internet Explorer HTML rendering engine to execute arbitrary code with the privileges of the user who viewed the HTML document. This vulnerability could be exploited to distribute viruses, worms, or other malicious code.

III. Solution

Apply a patch

Microsoft has released a cumulative patch for Internet Explorer that corrects this vulnerability and several others. For more information about the patch and the vulnerabilities, please see Microsoft Security Bulletin MS02-005:

<http://www.microsoft.com/technet/security/bulletin/MS02-005.asp>

Disable ActiveX Controls and Plugins

In Internet Explorer, plugins may be used to view, play, or otherwise process embedded objects. The execution of embedded objects is controlled by the "Run ActiveX Controls and Plugins" security option. Disabling this option will prevent embedded objects from being processed, and will therefore prevent exploitation of this vulnerability.

According to MS02-005:

The vulnerability could not be exploited if the "Run ActiveX Controls and Plugins" security option were disabled in the Security Zone in which the page was rendered. This is the default condition in the Restricted Sites Zone, and can be disabled manually in any other Zone.

At a minimum, disable the "Run ActiveX Controls and Plugins" security option in the Internet Zone and the zone used by Outlook or Outlook Express. The "Run ActiveX Controls and Plugins" security option is disabled in the "High" zone security setting. Instructions for configuring the Internet Zone to use the "High" zone security setting can be found in the CERT/CC Malicious Web Scripts FAQ:

http://www.cert.org/tech_tips/malicious_code_FAQ.html#steps

Apply the Outlook Email Security Update

Another way to effectively disable the processing of ActiveX controls and plugins in Outlook is to install the Outlook Email Security Update. The update configures Outlook to open email messages in the Restricted Sites Zone, where the "Run ActiveX Controls and Plugins" security option is disabled by default. In addition, the update provides further protection against malicious code that attempts to propagate via Outlook.

- Outlook 2002 and Outlook Express 6
The functionality of the Outlook Email Security Update is included in Outlook 2002 and Outlook Express 6.
- Outlook 2000
<http://office.microsoft.com/downloads/2000/Out2ksec.aspx>
- Outlook 98
<http://office.microsoft.com/downloads/9798/Out98sec.aspx>

Appendix A Vendor Information

This appendix contains information provided by vendors for this advisory. When vendors report new information to the CERT/CC, we update this section and note the changes in our revision history. If a particular vendor is not listed below, we have not received their comments.

Microsoft

Microsoft has released a Security Bulletin and a Knowledge Base Article addressing this vulnerability:

- Security Bulletin MS02-005
<http://www.microsoft.com/technet/security/bulletin/MS02-005.asp>
- Knowledge Base Article Q317731
<http://support.microsoft.com/default.aspx?scid=kb;en-us;Q317731>

Cyrusoft

Our email client Mulberry does not use the core HTML rendering engine library for its HTML display, and so is not affected by the bug in that library. Having looked at the details of this alert I can also confirm that our own HTML rendering engine is not affected by this, as it ignores the relevant tags.

Appendix B References

1. <http://www.kb.cert.org/vuls/id/932283>
2. <http://www.security.nnov.ru/advisories/mshtml.asp>
3. <http://www.microsoft.com/technet/security/bulletin/MS02-005.asp>
4. <http://support.microsoft.com/default.aspx?scid=kb;en-us;Q317731>
5. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0022>

6. <http://msdn.microsoft.com/workshop/author/dhtml/reference/objects/embed.asp>
7. <http://developer.netscape.com/docs/manuals/htmlguid/tags14.htm#1286379>

The CERT/CC thanks ERRor and DarkZorro of domain Hell and 3APA3A of SECURITY.NNOV for reporting this issue to us.

Author: Art Manion

Copyright 2002 Carnegie Mellon University

Revision History

February 25, 2002: Initial release

February 25, 2002: Fixed < and > tags

February 25, 2002: Updated Description with version information

March 5, 2002: Added MacOS and Unix information

April 2, 2002: Added AOL information

5 CA-2002-05: Multiple Vulnerabilities in PHP fileupload

Original release date: February 27, 2002

Last revised: --

Source: CERT/CC

A complete revision history can be found at the end of this file.

Systems Affected

- Web servers running PHP

Overview

Multiple vulnerabilities exist in the PHP scripting language. These vulnerabilities could allow a remote attacker to execute arbitrary code with the privileges of the PHP process.

I. Description

PHP is a scripting language widely used in web development. PHP can be installed on a variety of web servers, including Apache, IIS, Caudium, Netscape and iPlanet, OmniHTTPd and others. Vulnerabilities in the `php_mime_split` function may allow an intruder to execute arbitrary code with the privileges of the web server. For additional details, see

<http://security.e-matters.de/advisories/012002.html>

Web servers that do not have PHP installed are not affected by this vulnerability.

The CERT/CC is tracking this set of vulnerabilities as [VU#297363](#). At this time, these vulnerabilities have not been assigned a CVE identifier.

II. Impact

Intruders can execute arbitrary code with the privileges of the web server, or interrupt normal operations of the web server.

III. Solution

Apply a Patch

Upgrade to PHP version 4.1.2, available from

http://www.php.net/do_download.php?download_file=php-4.1.2.tar.gz

If upgrading is not possible, apply patches as described at <http://www.php.net/downloads.php>:

- For PHP 4.10/4.11
http://www.php.net/do_download.php?download_file=rfc1867.c.diff-4.1.x.gz
- For PHP 4.06
http://www.php.net/do_download.php?download_file=rfc1867.c.diff-4.0.6.gz
- For PHP 3.0
http://www.php.net/do_download.php?download_file=mime.c.diff-3.0.gz

If you are using version 4.20-dev, you are not affected by this vulnerability. Quoting from <http://security.e-matters.de/advisories/012002.htm>:

"[U]sers running PHP 4.2.0-dev from cvs are not vulnerable to any of the described bugs because the fileupload code was completely rewritten for the 4.2.0 branch."

Disable fileuploads

If upgrading is not possible or a patch cannot be applied, you can avoid these vulnerabilities by disabling fileupload support. Edit the PHP configuration file `php.ini` as follows:

```
file_uploads = off
```

Note that this setting only applies to version 4.0.3 and above. However, this will prevent you from using fileuploads, which may not be acceptable in your environment.

Appendix A Vendor Information

This appendix contains information provided by vendors for this advisory. When vendors report new information to the CERT/CC, we update this section and note the changes in our revision history. If a particular vendor is not listed below, we have not received their comments.

Apache Software Foundation

Information about this vulnerability is available from <http://www.php.net>

FreeBSD

FreeBSD does not include any version of PHP by default, and so is not vulnerable. However, the FreeBSD Ports Collection does contain both PHP3 and PHP4 packages. Updates to the PHP packages are in progress and corrected packages will be available in the near future.

MandrakeSoft

MandrakeSoft distributes PHP in all distributions and we are currently working on patching our versions of PHP for Linux-Mandrake 7.1 and 7.2; Mandrake Linux 8.0, 8.0/ppc, 8.1, and 8.1/ia64; Single Network Firewall 7.2; Corporate Server 1.0.1.

We anticipate having the updates out by the end of the week.

Microsoft

We do not use PHP in any products.

NCSA

NCSA does not include PHP as an add-in or bundled component in any products distributed.

Red Hat

Red Hat was notified of this issue on 27th February 2002. All supported versions of Red Hat Linux ship with PHP packages that are affected by these vulnerabilities. We will shortly be releasing errata packages which contain patched versions that are not vulnerable. The errata packages and our advisory will be available on our web site at the URL below. At the same time users of the Red Hat Network will be able to update their systems to patched versions using the up2date tool.

<http://www.redhat.com/support/errata/RHSA-2002-035.html>

The CERT Coordination Center thanks Stefan Esser, upon whose advisory this document is largely based.

Author: [Shawn V. Hernan](#)

Appendix B References

1. <http://www.kb.cert.org/vuls/id/297363>
2. <http://security.e-matters.de/advisories/012002.html>
3. http://www.iss.net/security_center/static/8281.php

Copyright 2002 Carnegie Mellon University

Revision History

February 27, 2002: Initial release

6 CA-2002-06: Vulnerabilities in Various Implementations of the RADIUS Protocol

Original release date: March 4, 2002

Last revised: April 16, 2002

Source: CERT/CC

A complete revision history can be found at the end of this file.

Systems Affected

Systems running any of the following RADIUS implementations:

- Ascend RADIUS versions 1.16 and prior
- Cistron RADIUS versions 1.6.5 and prior
- FreeRADIUS versions 0.3 and prior
- GnuRADIUS versions 0.95 and prior
- ICRADIUS versions 0.18.1 and prior
- Livingston RADIUS versions 2.1 and earlier
- Novell Border Manager
- Open System Consultants Radiator 2.6 and prior
- RADIUS (previously known as Lucent RADIUS) versions 2.1 and prior
- RADIUSClient versions 0.3.1 and prior
- Secure Computing Corp. SafeWord version 5.2 and SafeWord PremierAccess v3.0
- Vircom VOP Radius 3.2 and prior
- XTRADIUS 1.1-pre1 and prior
- YARD RADIUS 1.0.19 and prior

Overview

Remote Authentication Dial In User Service (RADIUS) servers are used for authentication, authorization and accounting for terminals that speak the RADIUS protocol. Multiple vulnerabilities have been discovered in several implementations of the RADIUS protocol.

I. Description

Two vulnerabilities in various implementations of RADIUS clients and servers have been reported to several vendors and the CERT/CC. They are remotely exploitable, and on most systems result in a denial of service. VU#589523 may allow the execution of code if the attacker has knowledge of the shared secret. Certain implementations vulnerable to VU#589523 may allow the execution of code if multiple packets are processed in the same thread, and the last 1 or 2 bytes of the shared secret is within a certain range.

VU#589523 - Multiple implementations of the RADIUS protocol contain a digest calculation buffer overflow

Multiple implementations of the RADIUS protocol contain a buffer overflow in the function that calculates message digests.

During the message digest calculation, a string containing the shared secret is concatenated with a packet received without checking the size of the target buffer. This makes it possible to overflow the buffer with shared secret data. This can lead to a denial of service against the server. If the shared secret is known by the attacker, then it may be possible to use this information to execute arbitrary code with the privileges of the victim RADIUS server or client, usually root. It should be noted that gaining knowledge of the shared secret is not a trivial task.

Certain implementations of RADIUS vulnerable to VU#589523 may allow the execution of code if multiple packets are processed in the same thread, and the last 1 or 2 bytes of the shared secret is within a certain range. In this case, specific knowledge of the shared secret is not required.

Systems Affected by VU#589523

- Ascend RADIUS versions 1.16 and prior
- Cistron RADIUS versions 1.6.4 and prior
- FreeRADIUS versions 0.3 and prior
- GnuRADIUS versions 0.95 and prior
- ICRADIUS versions 0.18.1 and prior
- Livingston RADIUS versions 2.1 and earlier
- Novell Border Manager
- RADIUS (commonly known as Lucent RADIUS) versions 2.1 and prior
- RADIUSClient versions 0.3.1 and prior
- Secure Computing Corp. SafeWord version 5.2 and SafeWord PremierAccess v3.0
- Vircom VOP Radius 3.2 and prior
- XTRADIUS 1.1-pre1 and prior
- YARD RADIUS 1.0.19 and prior

VU#936683 - Multiple implementations of the RADIUS protocol do not adequately validate the vendor-length of vendor-specific attributes.

Various RADIUS servers and clients permit the passing of vendor-specific and user-specific attributes. Several implementations of RADIUS fail to check the vendor-length of vendor-specific attributes. It is possible to cause a denial of service against RADIUS servers with a malformed vendor-specific attribute.

RADIUS servers and clients fail to validate the vendor-length inside vendor-specific attributes. The vendor-length shouldn't be less than 2. If vendor-length is less than 2, the RADIUS server (or client) calculates the attribute length as a negative number. The attribute length is then used in various functions. In most RADIUS servers the function that performs this calculation is rad_recv() or radrecv(). Some applications may use the same logic to validate user-specific attributes and be vulnerable via the same method.

Systems Affected by VU#936683

- Cistron RADIUS versions 1.6.5 and prior
- FreeRADIUS versions 0.3 and prior
- ICRADIUS versions 0.18.1 and prior
- Livingston RADIUS versions 2.1 and earlier
- Novell Border Manager
- Open System Consultants Radiator 2.6 and prior
- Secure Computing Corp. SafeWord version 5.2 and SafeWord PremierAccess v3.0
- XTRADIUS 1.1-pre1 and prior
- YARD RADIUS 1.0.19 and prior

II. Impact

Both of the vulnerabilities allow an attacker can cause a denial of service of the RADIUS server or client. On some systems, VU#589523 may allow the execution of code, especially if the attacker has knowledge of the shared secret.

III. Solution

Apply a patch, or upgrade to the version specified by your vendor.

Block packets to the RADIUS server at the firewall

Limit access to the RADIUS server to those addresses which are approved to authenticate to the RADIUS server. Note that this does not protect your server from attacks originating from these addresses.

Appendix A Vendor Information

This appendix contains information provided by vendors for this advisory. When vendors report new information to the CERT/CC, we update this section and note the changes in our revision history. If a particular vendor is not listed below, we have not received their comments.

Apple

Mac OS X and Mac OS X Server -- Not vulnerable since RADIUS is not shipped with those products.

Alcatel

Following the recent CERT advisory on security vulnerabilities in various RADIUS implementations, Alcatel has conducted an immediate assessment to determine any impact this may have on our portfolio. A first analysis has shown that the following products are not affected: Omni Switch/Routers, 713x VPN Gateways, A5735 SMC, A5020 SoftSwitch and GGSN. The security of our customers' networks is of highest priority for Alcatel. Therefore we continue to test our

product portfolio against potential RADIUS security vulnerabilities and will provide updates if necessary.

Athena Online

It is our pleasure to report that Athena Online's Radicate RADIUS server is not vulnerable to CERT RADIUS VU#936683 and VU#589523 in our internal testing.

Radicade has been written from the ground up following the RFCs, using no previously existing code. Security issues such as buffer overflows have been identified and taken care of at each and every state of development to prevent any denial of service or execution of foreign code.

Radicade runs on a variety of platforms, including (but not limited to) Mac OS X, Mac OS X Server, Mac OS 9, Solaris, Linux and Win32.

Cisco

Cisco Systems has reviewed the following products that implement RADIUS with regards to this vulnerability, and has determined that the following are NOT vulnerable to this issue; Cisco IOS, Cisco Catalyst OS, Cisco Secure PIX firewall, Cisco Secure Access Control System for Windows, Cisco Aironet, Cisco Access Registrar, and Cisco Resource Pooling Management Service. At this time, we are not aware of any Cisco products that are vulnerable to the issues discussed in this report.

Cistron

You state 2 vulnerabilities:

1. Digest Calculation Buffer Overflow Vulnerability Cistron Radius up to and including 1.6.4 is vulnerable
2. Invalid attribute length calculation on malformed Vendor-Specific attr. Cistron Radius up to and including 1.6.5 is vulnerable

Today I have released version 1.6.6, which also fixes (2). The homepage is <http://www.radius.cistron.nl/> on which you can also find the ChangeLog. An announcement to the cistron-radius mailinglist was also made today.

So everybody should upgrade to 1.6.6.

Conectiva

See <http://distro.conectiva.com.br/atualizacoes/?id=a&anuncio=000466>

FreeBSD

FreeBSD versions prior to 4.5-RELEASE (which is shipping today or tomorrow or so) do contain some of the RADIUS packages mentioned below: radiusd-cistron, freeradius, ascend-radius, icradius, and radiusclient. However, 4.5-RELEASE will not ship with any of these RADIUS packages, except radiusclient. Also, note that the information you [CERT/CC] have forwarded previously indicates that neither Merit RADIUS (radius-basic) nor radiusclient are vulnerable.

Fujitsu

Fujitsu's UXP/V operating system is not vulnerable because UXP/V does not support the Radius functionality.

Funk Software

See http://www.funk.com/News&Events/CERT_resp.asp

GnuRADIUS

The bug was fixed in version 0.96.

Hewlett-Packard

We have tested our Version of RADIUS, and we are NOT vulnerable.

IBM

IBM's AIX operating system, all versions, is not vulnerable as we do not ship the RADIUS project with AIX.

Interlink Networks

Interlink Networks has inspected and tested all released versions of its RADIUS server for susceptibility to the issues described in VU#936683 and VU#589523. NONE of Interlink Networks products are susceptible to the vulnerabilities outlined in the advisory.

Interlink Networks also inspected and tested Merit RADIUS server version 3.6B2 and found that it is NOT vulnerable to the reported issues.

Juniper Networks

Juniper products have been tested and are not affected by this vulnerability.

Lucent Technologies, Inc.

Lucent and Ascend "Free" RADIUS server Product Status

Prior to the Lucent Technologies acquisition of Ascend Communications and Livingston Enterprises, both companies distributed RADIUS servers at no cost to their customers. The initial Livingston server was RADIUS 1.16 followed in June 1999 by RADIUS 2.1. The Ascend server was based on the Livingston 1.16 product with the most recent version being released in June 1998. Lucent Technologies no longer distributes these products, and does not provide any support services for these products.

Both of these products were distributed as-is without warranty, under the BSD "Open Source" license. Under this license, other parties are free to develop and release other products and versions. However, as noted in the license terms, Lucent Technologies can not and does not assume any responsibility for any releases, present or future, based on these products.

Product Patches

Patches designed to specifically address the problems outlined in the CERT bulletins VU#936683 VU#589523 have been made available to the public by Simon Horman . For more information visit <ftp://ftp.vergenet.net/pub/radius>

Replacement Product

The Lucent Technologies replacement product is NavisRadius 4.x. NavisRadius is a fully supported commercial product. Visit the product web site at <http://www.lucentradius.com> for more information.

Richard Perlman
NavisRadius Product Management
Network Operations Software
perl@lucent.com

Microsoft

We've completed our investigation into this issue based on the information provided and have determined that no version of Microsoft IAS is susceptible to either vulnerability.

NetBSD

Some of the affected radius daemons are available from NetBSD pkgsrc. It is highly advisable that you update to the latest versions available from pkgsrc. Also note that pkgsrc/security/audit-packages can be used to notify you when new pkgsrc related security issues are announced.

Novell

Novell's RADIUS server (Border Manager) is only vulnerable to administrator-installed shared secrets and VSAs. We are assessing this vulnerability in more detail.

Open System Consultants

The current version of Radiator (2.19) is not vulnerable to either of the vulnerabilities reported. No version has ever been vulnerable to VU#589523, and it has not been vulnerable to VU#936683 since version 2.6 (released on 5/4/1998)

More information in our press release at

<http://www.open.com.au/press.html>

Process Software

MultiNet and TCPware do not provide a RADIUS implementation.

RADIUS (previously known as Lucent RADIUS)

I wish to advise that Lucent Radius 2.1 is vulnerable to VU#589523, but is not vulnerable to VU#936683.

I have made an unofficial patch to this code to resolve this problem. It will be released in <ftp://ftp.vergenet.net/pub/radius/> where previous patches to Radius by myself are available.

RADIUSClient

I've just uploaded version 0.3.2 of the radiusclient library to <ftp://ftp.cityline.net/pub/radiusclient/radiusclient-0.3.2.tar.gz> which contains a fix for the reported buffer overflow.

Red Hat

We do not ship any radius software as part of any of our main operating system. However, Cistron RADIUS was part of our PowerTools add-on software CD from versions 5.2 through 7.1. Thus while not installed by default, some users of Red Hat Linux may be using Cistron RADIUS. Errata packages that fix this problem and our advisory will be available shortly on our web site at the URL below. At the same time users of the Red Hat Network will be able to update their systems to patched versions using the up2date tool.

<http://www.redhat.com/support/errata/RHSA-2002-030.html>

Riverstone Networks

Riverstone Networks products have been tested and are not affected by the vulnerabilities listed in VU#589523.

SCO

The Caldera NON-Linux operating systems: OpenServer, UnixWare, and Open UNIX, do not ship Radius servers or clients.

Secure Computing Corporation

Secure Computing has provided updated RADIUS daemons for the following SafeWord systems running on Solaris: SafeWord v5.2, and SafeWord PremierAccess v3.0. The new updated daemon addresses the following vulnerabilities as was reported in the CERT Advisory CA-2002-06:

VU#589523

Previously, the radiusd daemon contained a buffer overflow in the function that calculates message digest, and the daemon would crash when a secret key of more than 108 characters was entered in the clients file. The new version will now display the following radius debug message when such a key exists:

"ERROR! Calc_digest: Bad secret key in clients file. Length is too long."

The daemon will remain running.

VU#936683

Previously, the radiusd daemon would crash when malformed RADIUS packets that included Vendor Specific Attributes of lengths of less than 2 bytes. This version will now display the following radius debug message in this situation:

"Invalid attribute. Invalid length for attribute 26."

The daemon will remain running.

To obtain the new updated RADIUS daemon, please contact Secure Computing Technical support at 1-800-700-8328

SGI

SGI does not ship with a RADIUS server or client, so we are not vulnerable to these issues.

Vircom Inc.

See <http://www.vircom.com/solutions/vopradius/certadvisoryca200206.htm>

Wind River Systems

The current RADIUS client product from Wind River Systems, WindNet RADIUS 1.1, is not susceptible to VU#936683 and VU#589523 in our internal testing.

VU#936683 - WindNet RADIUS will pass the packet up to the application. The application may need to be aware of the invalid attribute length.

VU#589523 - WindNet RADIUS will drop the packet overflow.

Please contact Wind River support at support@windriver.com or call (800) 458-7767 with any test reports related to VU#936683 and VU#589523.

XTRADIUS

We are trying to release a new and fixed version of xtradius by the end of the month (version 1.2.1).. Right now the new version is on the CVS and we are testing it...

YARD RADIUS

Current version 1.0.19 of Yardradius (which is derived from Lucent 2.1) seems suffering both the problems. I think I will release a new version (1.0.20) which solves those buffer overflows before your suggested date [3/4/2002].

Our thanks to 3APA3A <3APA3A@security.nnov.ru> and Joshua Hill and for their cooperation, reporting and analysis of this vulnerability.

Feedback about this Advisory can be sent to the author, Jason A. Rafail.

Appendix B References

1. <http://www.kb.cert.org/vuls/id/589523>
2. <http://www.kb.cert.org/vuls/id/936683>
3. <http://www.security.nnov.ru/advisories/radius.asp>
4. <http://www.untruth.org/~josh/security/radius>
5. <http://www.securityfocus.com/bid/3530>

Copyright 2002 Carnegie Mellon University

Revision History

March 04, 2002: Initial release
March 05, 2002: Updated Lucent Statement
March 12, 2002: Added Athena Online's Statement
March 12, 2002: Updated the description for VU#589523
March 12, 2002: Added Open System Consultants Statement
March 13, 2002: Added Riverstone Networks Statement
March 18, 2002: Added Interlink Networks Statement
March 28, 2002: Updated the impact on RADIUS clients
March 28, 2002: Added Funk Software Statement
April 02, 2002: Added Alcatel Statement
April 02, 2002: Added Vircom Statement
April 12, 2002: Added Novell Statement
April 16, 2002: Added Secure Computing Corporation Statement

7 CA-2002-07: Double Free Bug in zlib Compression Library

Original release date: March 12, 2002

Last revised: July 20, 2002

Source: CERT/CC

A complete revision history can be found at the end of this file.

Systems Affected

- Any software that is linked to zlib 1.1.3 or earlier may be affected
- Data compression libraries derived from zlib 1.1.3 or earlier may contain a similar bug

Overview

There is a bug in the zlib compression library that may manifest itself as a vulnerability in programs that are linked with zlib. This may allow an attacker to conduct a denial-of-service attack, gather information, or execute arbitrary code.

It is important to note that the CERT/CC has not received any reports of exploitation of this bug. Based on the information available to us at this time, it is difficult to determine whether this bug can be successfully exploited. However, given the widespread deployment of zlib, we have published this document as a proactive measure.

I. Description

There is a bug in the decompression algorithm used by the popular zlib compression library. If an attacker is able to pass a specially-crafted block of invalid compressed data to a program that includes zlib, the program's attempt to decompress the crafted data can cause the zlib routines to corrupt the internal data structures maintained by malloc.

The bug results from a programming error that causes segments of dynamically allocated memory to be released more than once (i.e., "double-freed"). Specifically, when `inftrees.c:huft_build()` encounters the crafted data, it returns an unexpected `Z_MEM_ERROR` to `inftrees.c:inflate_trees_dynamic()`. When a subsequent call is made to `infblock.c:inflate_blocks()`, the `inflate_blocks` function tries to free an internal data structure a second time.

Because this bug interferes with the proper allocation and deallocation of dynamic memory, it may be possible for an attacker to influence the operation of programs that include zlib. In most circumstances, this influence will be limited to denial of service or information leakage, but it is theoretically possible for an attacker to insert arbitrary code into a running program. This code would be executed with the permissions of the vulnerable program.

The CERT/CC is tracking this issue as [VU#368819](#). This reference number corresponds to [CVE](#) candidate [CAN-2002-0059](#).

II. Impact

This bug may introduce vulnerabilities into any program that includes the affected library. Depending upon how and where the zlib routines are called from the given program, the resulting vulnerability may have one or more of the following impacts: denial of service, information leakage, or execution of arbitrary code.

III. Solution

Upgrade your version of zlib

The maintainers of zlib have released version 1.1.4 to address this vulnerability. Upgrade any software that is linked to or derived from an earlier version of zlib. The latest version of zlib is available at <http://www.zlib.org>

These are the MD5 checksums for zlib version 1.1.4:

```
abc405d0bdd3ee22782d7aa20e440f08 zlib-1.1.4.tar.gz  
9bf1d36ced334b0cf1f996f5c8171018 zlib114.zip
```

The maintainers of zlib have published an advisory regarding this issue; for further information, please see

<http://www.gzip.org/zlib/advisory-2002-03-11.txt>

Apply a patch from your vendor

The zlib compression library is freely available and used by many vendors in a wide variety of applications. Any one of these applications may contain vulnerabilities that are introduced by this vulnerability.

[Appendix A](#) contains information provided by vendors for this advisory. As vendors report new information to the CERT/CC, we will update this section and note the changes in our revision history. If a particular vendor is not listed below, we have not received their comments. Please contact your vendor directly.

Appendix A Vendor Information

This appendix contains information provided by vendors for this advisory. As vendors report new information to the CERT/CC, we will update this section and note the changes in our revision history. If a particular vendor is not listed below, we have not received their comments.

Apple Computer, Inc.

Mac OS X and Mac OS X Server do not contain this vulnerability.

Cisco Systems

Cisco Systems is addressing the vulnerability identified by VU#368819 across all affected products. Cisco has released an advisory:

<http://www.cisco.com/warp/public/707/zlib-double-free.shtml>

Compaq Computer Corporation

COMPAQ COMPUTER CORPORATION

x-ref: SSRT0818 zlib

At the time of writing this document, Compaq continues to evaluate this potential problem and impacts to Compaq released software. Compaq will implement solutions based on the conclusion of this evaluation as necessary. Compaq will provide notice of any new patches as a result any required solution through standard patch notification procedures and be available from your normal Compaq Services support channel.

COMPAQ COMPUTER CORPORATION

Conectiva Linux

Conectiva Linux supported versions (5.0, 5.1, 6.0, 7.0, ferramentas graficas and ecommerce) are affected by the zlib vulnerability. Updates will be sent to our security mailing lists and be available at our ftp site and mirrors. The updates will include a new version of zlib itself and also other packages which include their own version of zlib or are linked statically to the system-wide copy of zlib.

Debian

Users of Debian GNU/Linux 2.2 (potato) should upgrade to zlib version 1.1.3-5.1. More information is available at <http://www.debian.org/security/2002/dsa-122>. Note that a few packages which include private copies of zlib will also need to be upgraded--more information is available at the above link.

Engarde

EnGarde Secure Linux Community and Professional are both vulnerable to the zlib bugs. Guardian Digital addressed this vulnerability in ESA-20020311-008 which may be found at:

http://www.linuxsecurity.com/advisories/other_advisory-1960.html

EnGarde Secure Professional users may upgrade their systems using the Guardian Digital Secure Network.

FreeBSD

FreeBSD is not vulnerable, as the FreeBSD malloc implementation detects and complains about several programming errors including this kind of double free.

F-Secure Corporation

F-Secure SSH is not vulnerable to zlib double free bug.

No version of F-Secure SSH software is vulnerable to the "Double Free Bug in zlib Compression Library" discussed in CERT Advisory CA-2002-07.

All F-Secure SSH versions, both the old SSH1 and later SSH2 protocol clients and servers, close connection immediately with fatal cleanup call without any further calls to zlib when call to zlib's inflate() returns something else than Z_OK.

Fujitsu

Fujitsu's UXP/V operating system is not affected by the zlib vulnerability because it does not support zlib.

Hewlett-Packard Company

Some HP-UX software (for example, X and lbxproxy) is linked with the 1.0.8 version of zlib. This version came before the introduction of the reported double free problem and is not vulnerable.

Other HP-UX software (for example, OpenSSH) is linked with the latest zlib (1.1.4) and is not vulnerable.

IBM Corporation

IBM's AIX operating system, version 5.1, ships with open source-originated zlib that is used with the Red Hat Package Manager (rpm) to install applications that are included in the AIX-Linux Affinity Toolkit. zlib (libz.a) is a shared library in AIX. AIX 5.1 is presumed susceptible to the described vulnerability, though we have not demonstrated exploitability yet. AIX 4.3.x does not ship with zlib, but customers who install zlib and use it may be similarly vulnerable.

The updated zlib package can be downloaded by directing your browser to:

<http://oss.software.ibm.com/developerworks/projects/aixtoolbox>

The updated rpm package can be downloaded from:

<ftp://ftp.software.ibm.com/aix/freeSoftware/aixtoolbox/INSTALLP/ppc/rpm.rte>

Juniper Networks

Juniper Networks has completed an initial assessment of this vulnerability, and we believe that our implementation is not susceptible. Test programs show that our memory allocation algorithm correctly detects and warns about any attempt to exploit the vulnerability described in the CERT/CC advisory.

We continue to evaluate the risks associated with this vulnerability. If we determine that the JUNOS software is susceptible, we will quickly issue any patches or software updates required to maintain the security of Juniper Networks routers.

Future JUNOS software releases will include a corrected version of the libz code.

Microsoft Corporation

Microsoft conducted a thorough source-code level review of its products in response to the reports of vulnerabilities in zlib. This review did not discover any vulnerabilities related to these reports.

NetBSD

NetBSD's malloc libraries are not vulnerable to double-free() attacks. The updated zlib will be included in future releases, but a Security Advisory will not be issued.

Novell, Inc.

Novell is working on a fix for Novell JVM for NetWare 1.3.1. We will post the fix in the May NDK. Version 1.4 will also have the fix in it. We will also update this statement with the URL to download the fix.

OpenBSD

OpenBSD is not vulnerable as OpenBSD's malloc implementation detects double freeing of memory. The zlib shipped with OpenBSD has been fixed in OpenBSD-current in January 2002.

OpenSSH

OpenSSH itself relies on zlib as a third party library. OpenSSH's internal malloc state might get corrupted if the double-free bug is present in zlib. At this moment, it is not known if this bug will allow an intruder to gain privileges.

For some malloc implementation it is possible to detect and ignore the double-free. However, that is entirely dependent on the malloc implementation. Currently, it seems that *BSD operating systems might not be affected by this problem.

We advise everybody to upgrade their third party libraries and recompile OpenSSH if necessary. Turning off compression in the server is possible only by removing zlib from myproposal.h and subsequent recompilation.

Index: myproposal.h

```

=====
RCS file: /cvs/src/usr.bin/ssh/myproposal.h,v
retrieving revision 1.13
diff -u -r1.13 myproposal.h
--- myproposal.h 21 Jan 2002 22:30:12 -0000 1.13
+++ myproposal.h 12 Mar 2002 17:36:11 -0000
@@ -32,7 +32,7 @@
    "hmac-md5,hmac-sha1,hmac-ripemd160," \
    "hmac-ripemd160@openssh.com," \
    "hmac-sha1-96,hmac-md5-96"
-#define KEX_DEFAULT_COMP "none,zlib"
!)+#define KEX_DEFAULT_COMP "none"
#define KEX_DEFAULT_LANG ""

```

Openwall GNU/*/Linux

All versions of Openwall GNU/*/Linux (Owl) prior to the 2002/02/15 Owl-current snapshot are affected by the zlib double-free vulnerability. Owl-current after 2002/02/15 includes the proper fixes in its userland packages. In order to not place the users of other vendors' products at additional risk, we have agreed to delay documenting this as a security change and including the fixes in Owl 0.1-stable until there's a coordinated public announcement. While we don't normally support this kind of a policy (releasing a fix before there's an announcement), this time handling the vulnerability in this way was consistent with the state of things by the time the (already publicly known) bug was first realized to be a security vulnerability.

The zlib bug could affect the following Owl packages: gnupg, openssh, rpm, texinfo (not necessarily in a security sense). Of these, the OpenSSH could potentially allow for an active remote attack resulting in a root compromise. If only SSH protocol version 1 is allowed in the OpenSSH server this is reduced to a local attack, but reverse remote attack possibilities by a malicious server remain. Additionally, any third-party software that makes use of the provided zlib library could be affected.

Parts of the Linux 2.2 kernel included in Owl were also affected by the vulnerability. Fortunately, those parts (Deflate compression support for PPP and the experimental Deflate compression extension to IrDA) are normally not used by the Owl userland. The bug has been corrected starting with Linux 2.2.20-ow2 which has been made public and a part of both Owl-current and Owl 0.1-stable on 2002/03/03. This change, however, will only be documented in the publicly-available change logs on the coordinated public announcement date.

Red Hat, Inc.

Red Hat Linux ships with a zlib library that is vulnerable to this issue. Although most packages in Red Hat Linux use the shared zlib library we have identified a number of packages that either statically link to zlib or contain an internal version of the zlib code.

Updates to zlib and these packages as well as our advisory note are available from the following URL. Users of the Red Hat Network can use the up2date tool to automatically upgrade their systems.

<http://www.redhat.com/support/errata/RHSA-2002-026.html>

Red Hat would like to thank CERT/CC for their help in coordinating this issue with other vendors.

SGI

SGI acknowledges the zlib vulnerabilities reported by CERT and is currently investigating. No further information is available at this time.

For the protection of all our customers, SGI does not disclose, discuss or confirm vulnerabilities until a full investigation has occurred and any necessary patch(es) or release streams are available for all vulnerable and supported IRIX operating systems. Until SGI has more definitive information to provide, customers are encouraged to assume all security vulnerabilities as exploitable and take appropriate steps according to local site security policies and requirements. As further information becomes available, additional advisories will be issued via the normal SGI security information distribution methods including the wiretap mailing list on <http://www.sgi.com/support/security/>.

SSH Communications Security

SSH Secure Shell is not vulnerable to zlib double free bug.

No version of SSH Secure Shell software is vulnerable to the "Double Free Bug in zlib Compression Library" discussed in CERT Advisory CA-2002-07.

All SSH Secure Shell versions, including SSH2 protocol clients and servers, close the connection immediately with a fatal cleanup call without any further calls to zlib when a call to zlib's inflate() returns something else than Z_OK.

Standard Networks, Inc.

Standard Networks offers a "mainframe connectivity" product called "OpenIT" which uses the zlib library to compress ("zip") files transferred between Unisys mainframes and remote FTP clients and servers. After a code analysis we found the zlib vulnerability does not affect this product.

Standard Networks also offers a secure HTTPS-based file transfer client called "MOVEit Wizard" which uses the zlib library to compress ("zip") files transferred between MOVEit DMZ servers

and remote browsers. After a code analysis we found the zlib vulnerability does not affect this product.

Nonetheless, Standard Networks will use "corrected" versions of zlib in future versions of both products.

No other Standard Networks products ("ActiveHEAT", "EMU", "MOVEit DMZ", "MOVEit Central", "MOVEit Admin", "MOVEit Freely", "MOVEit Buddy", "Unigate") are affected.

Customers are encouraged to call Standard Networks immediately (+001 608.227.6100) with any questions or concerns about their specific configuration.

Sun Microsystems, Inc.

Solaris 8 includes the zlib library as part of the SUNWzlib package which is affected by this issue. Open Windows 3.6.1 (for Solaris 7) and Open Windows 3.6.2 (for Solaris 8) ship a version of zlib which is affected in recent patches. Sun has produced patches for both Solaris and Open Windows which address this issue. The impact and patch details are described in Sun Alert 43541 available here:

<http://sunsolve.Sun.COM/pub-cgi/retrieve.pl?doc=fsalert%2F43541>

SuSE Linux AG

All SuSE Linux versions previous to 8.0 are affected by this issue. We have released security updates for zlib itself, as well as several packages including their own copy of zlib.

Details on this issue, as well as the list of packages to upgrade, can be found in our advisory at:

http://www.suse.de/de/support/security/2002_010_libz_txt.html

http://www.suse.de/de/support/security/2002_011_libz_packages_txt.html

XFree86

XFree86 versions 4.0 through 4.2.0 include zlib version 1.0.8. XFree86 3.x includes zlib version 1.0.4. The zlib code included with XFree86 is only used on some platforms. This is determined by the setting of HasZlib in the imake config files in the xc/config/cf source directory. If HasZlib is set to YES in the platform's vendor.cf file(s), then the system-provided zlib is used instead of the XFree86-provided version. XFree86 uses the system-provided zlib by default only on the following platforms:

FreeBSD 2.2 and later
NetBSD 1.2.2 and later
OpenBSD
Darwin
Debian Linux

The zlib code in XFree86 has been fixed in the CVS repository (trunk and the xf-4_2-branch branch) as of 14 February 2002. A source patch for XFree86 4.2.0 will be available from <ftp://ftp.xfree86.org/pub/XFree86/4.2.0/fixes/>.

The following XFree86 4.2.0 binary distributions provided by XFree86 include and use a vulnerable version of zlib:

Linux-alpha-glibc22

Linux-ix86-glibc22

When updated binaries are available, it'll be documented at <http://www.xfree86.org/4.2.0/UPDATES.html>.

To check if an installation of XFree86 includes zlib, see if the following file exists:

`/usr/X11R6/lib/libz.a`

To check if an XFree86 X server is dynamically linked with zlib, look for a line containing 'libz' in the output of `'ldd /usr/X11R6/bin/XFree86'`.

Various vendors repackage and distribute XFree86, and may use settings and configurations different from those described here.

zlib.org

All users of zlib versions 1.1.3 or earlier should obtain the latest version, 1.1.4 or later, from <http://www.zlib.org>, in order to avoid this vulnerability as well as other possible vulnerabilities in versions prior to 1.1.3 when decompressing invalid data.

Appendix B References

- http://bugzilla.gnome.org/show_bug.cgi?id=70594
- <http://www.gzip.org/zlib/advisory-2002-03-11.txt>
- <http://www.kb.cert.org/vuls/id/368819>
- <http://www.libpng.org/pub/png/pngapps.html>
- <http://www.redhat.com/support/errata/RHSA-2002-026.html>
- <http://www.securityfocus.com/bid/4267>

The CERT/CC thanks Owen Taylor and Mark Cox of Red Hat, Inc. for reporting this vulnerability. We also thank Mark Adler of zlib.org for contributing to our research and Matthias Clasen for contributing to the discovery of this vulnerability.

This document was written by [Jeffrey P. Lanza](#).

Copyright 2002 Carnegie Mellon University

Revision History

Mar 12, 2002: Initial release

Mar 14, 2002: Added references to zlib advisory
Mar 15, 2002: Added Microsoft statement
Mar 15, 2002: Added NetBSD statement
Mar 15, 2002: Added F-Secure statement
Mar 18, 2002: Added Debian statement
Mar 18, 2002: Added Standard Networks statement
Mar 21, 2002: Added SSH Communications statement
Mar 21, 2002: Added Sun Microsystems statement
Mar 29, 2002: Added Juniper Networks statement; updated Hewlett-Packard statement
Apr 03, 2002: Added Cisco statement
Apr 14, 2002: Added Novell statement; updated Hewlett-Packard statement
May 02, 2002: Updated Microsoft statement
May 06, 2002: Added SuSE Linux AG statement
Jun 17, 2002: Updated Sun Microsystems statement
Jun 24, 2002: Added OpenSSH statement
Jun 25, 2002: Updated IBM statement
Jul 20, 2002: Updated Hewlett-Packard statement

8 CA-2002-08: Multiple Vulnerabilities in Oracle Servers

Original release date: March 14, 2002

Last revised: September 17, 2002

Source: CERT/CC

A complete revision history can be found at the end of this file.

Systems Affected

- Systems running Oracle9i Application Server
- Systems running Oracle9i Database
- Systems running Oracle8i Database

Overview

Multiple vulnerabilities in Oracle Application Server and Oracle Database have recently been discovered. These vulnerabilities include buffer overflows, insecure default settings, failures to enforce access controls, and failure to validate input. The impacts of these vulnerabilities include the execution of arbitrary commands or code, denial of service, and unauthorized access to sensitive information.

I. Description

Oracle Application Server includes a web server based on the Apache HTTP Server. Oracle extends the web server with a variety of different components that can be used provide interfaces to database applications. These components include, but are not limited to, a Procedural Language/Structured Query Language (PL/SQL) module, Java Server Pages, XSQL Servlets, and Simple Object Access Protocol (SOAP) applications. A number of vulnerabilities have been reported in these and other components used in Oracle Application Server and Oracle Database.

Although these reports focus primarily on Oracle9i Application Server, Oracle Database products are also affected. In particular, vulnerable versions of the PL/SQL module can be used with Oracle9i Application Server, Oracle9i Database, and Oracle8i Database.

The vulnerabilities referenced in this advisory were reported in several publications by David Litchfield of NGSSoftware:

- Hackproofing Oracle Application Server
<http://www.nextgenss.com/papers/hpoas.pdf>
- NGSSoftware Insight Security Research Advisory #NISR20122001
<http://www.nextgenss.com/advisories/plsql.txt>
- NGSSoftware Insight Security Research Advisory #NISR06022002A
<http://www.nextgenss.com/advisories/oraplsxtproc.txt>

- NGSSoftware Insight Security Research Advisory #NISR06022002B
<http://www.nextgenss.com/advisories/oraplsbos.txt>
- NGSSoftware Insight Security Research Advisory #NISR06022002C
<http://www.nextgenss.com/advisories/orajsa.txt>
<http://www.nextgenss.com/advisories/orajsp.txt>

For the complete list of Oracle-related vulnerabilities published by the CERT/CC, please search the [Vulnerability Notes Database](#) using the term "Oracle". Details about specific vulnerabilities can be found in the appropriate Vulnerability Note.

Buffer overflows

Several buffer-overflow vulnerabilities exist in the way the PL/SQL module handles HTTP requests and configuration parameters. Default configuration settings in a range of components are insecure, and different components fail to apply access restrictions uniformly. These vulnerabilities expose both the systems running Oracle Application Server and the information held in the underlying databases to undue risk.

Two more buffer overflow vulnerabilities exist in code that processes configuration parameters. These parameters processes configuration parameters that can be specified via the PL/SQL gateway web administration interface. By default, access to the PL/SQL gateway web administration interface is not restricted [[VU#611776](#)].

[VU#500203](#) - Oracle9i Application Server Apache PL/SQL module vulnerable to buffer overflow via help page request

[VU#313280](#) - Oracle9i Application Server Apache PL/SQL module vulnerable to buffer overflow via HTTP Location header

[VU#750299](#) - Oracle9i Application Server Apache PL/SQL module vulnerable to buffer overflow via HTTP request

[VU#878603](#) - Oracle9i Application Server Apache PL/SQL module vulnerable to buffer overflow via HTTP Authorization header

[VU#659043](#) - Oracle9i Application Server Apache PL/SQL module vulnerable to buffer overflow via Database Access Descriptor password

[VU#923395](#) - Oracle9i Application Server Apache PL/SQL module vulnerable to buffer overflow via cache directory name

Insecure default configurations

The default installation of Oracle Application Server includes a number of insecure configuration settings, such as well-known default passwords and unrestricted access to applications and sensitive information.

[VU#307835](#) - Oracle9i Application Server OWA_UTIL procedures expose sensitive information

VU#736923 - Oracle 9iAS SOAP components allow anonymous users to deploy applications by default

VU#611776 - Oracle9i Application Server PL/SQL Gateway web administration interface uses null authentication by default

VU#698467 - Oracle 9iAS default configuration allows access to "globals.jsa" file

VU#476619 - Oracle 9iAS default configuration allows arbitrary users to view sensitive configuration files

VU#712723 - Oracle 9iAS default configuration uses well-known default passwords

VU#168795 - Oracle 9iAS allows anonymous remote users to view sensitive Apache services by default

VU#278971 - Oracle 9i Application Server does not adequately handle requests for nonexistent JSP files thereby disclosing web folder path information

Failure to enforce access controls

Oracle Application Server does not uniformly enforce access restrictions. Different components do not adequately check authorization before granting access to protected resources.

VU#180147 - Oracle 9i Database Server PL/SQL module allows remote command execution without authentication

VU#193523 - Oracle9i Application Server allows unauthenticated access to PL/SQL applications via alternate Database Access Descriptor

VU#977251 - Oracle 9iAS XSQL Servlet ignores file permissions allowing arbitrary users to view sensitive configuration files

VU#547459 - Oracle 9iAS creates temporary files when processing JSP requests that are world-readable

Failure to validate input

In one case, the PL/SQL module does not properly handle a malformed HTTP request.

VU#805915 - Oracle9i Application Server Apache PL/SQL module does not properly handle HTTP Authorization header

II. Impact

The impacts of these vulnerabilities include the remote execution of arbitrary code, remote execution of commands and SQL queries, disclosure of sensitive information, and denial of service.

Remote execution of arbitrary commands and code

This section contains vulnerabilities that permit a remote intruder to cause a denial of service or execute arbitrary commands, code, or queries on the system.

Some of these vulnerabilities allow execution with the privileges of the Apache process. On UNIX systems, the Apache process typically runs as the "oracle" user. On Windows systems, the Apache service typically runs as the SYSTEM user; therefore, an attacker could gain complete control of the system by exploiting these vulnerabilities.

VU#500203 - Oracle9i Application Server Apache PL/SQL module vulnerable to buffer overflow via help page request

VU#313280 - Oracle9i Application Server Apache PL/SQL module vulnerable to buffer overflow via help page request Location: header

VU#750299 - Oracle9i Application Server Apache PL/SQL module vulnerable to buffer overflow via HTTP request

VU#878603 - Oracle9i Application Server Apache PL/SQL module vulnerable to buffer overflow via HTTP Authorization header password parameter

VU#659043 - Oracle9i Application Server Apache PL/SQL module vulnerable to buffer overflow via Database Access Descriptor password

VU#923395 - Oracle9i Application Server Apache PL/SQL module vulnerable to buffer overflow via cache directory name

VU#180147 - Oracle 9i Database Server PL/SQL module allows remote command execution without authentication

VU#736923 - Oracle 9iAS SOAP components allow anonymous users to deploy applications by default

VU#712723 - Oracle 9iAS default configuration uses well-known default passwords

VU#611776 - Oracle9i Application Server PL/SQL Gateway web administration interface uses null authentication by default

Unauthorized access to sensitive information

A number of vulnerabilities disclose configuration information or expose data stored in underlying databases. Also, insecure applications could allow an intruder to execute SQL queries. Oracle system programmers may wish to examine these vulnerabilities in Oracle's sample pages to prevent similar vulnerabilities in their own Oracle applications.

VU#307835 - Oracle9i Application Server OWA_UTIL PL/SQL application exposes procedures that are remotely accessible by arbitrary users

VU#193523 - Oracle 9i Application Server allows unauthenticated access to PL/SQL applications via alternate Database Access Descriptor

VU#698467 - Oracle 9iAS default configuration allows access to "globals.jsa" file

VU#476619 - Oracle 9iAS default configuration allows arbitrary users to view sensitive configuration files

VU#977251 - Oracle 9iAS XSQL Servlet ignores file permissions allowing arbitrary users to view sensitive configuration files

VU#168795 - Oracle 9iAS allows anonymous remote users to view sensitive Apache services by default

VU#278971 - Oracle 9i Application Server does not adequately handle requests for nonexistent JSP files thereby disclosing web folder path information

VU#547459 - Oracle 9iAS creates temporary files when processing JSP requests that are world-readable

Denial of service

In the case where the PL/SQL module does not properly handle an HTTP request, a denial-of-service vulnerability exists. Also, an unsuccessful attempt to exploit a buffer overflow vulnerability could crash the Apache service.

VU#805915 - Oracle9i Application Server Apache PL/SQL module does not properly handle HTTP Authorization header

III. Solution

Oracle has provided patches and workarounds that address most of these vulnerabilities. Sites using Oracle Application Server are encouraged to install the appropriate patches and make the recommended configuration changes provided by Oracle.

Solutions and workarounds for specific vulnerabilities can be found in individual Vulnerability Notes and in the following Oracle security alerts:

- Oracle Security Alert #29
http://otn.oracle.com/deploy/security/pdf/plsxtproc_alert.pdf
- Oracle Security Alert #28
http://otn.oracle.com/deploy/security/pdf/ias_modplsql_alert.pdf
- Oracle Security Alert #25
<http://otn.oracle.com/deploy/security/pdf/modplsql.pdf>
- Oracle Security Alert #22
http://otn.oracle.com/deploy/security/pdf/ias_soap_alert.pdf

Security and patch information for Oracle products are available at the following locations:

- Oracle Security Alerts
<http://otn.oracle.com/deploy/security/alerts.htm>
- MetaLink (registration required)
<http://metalink.oracle.com/>

Sites using Oracle Application Server may also find David Litchfield's *Hackproofing Oracle Application Server* paper useful in describing the impacts and various interactions of these vulnerabilities.

Apply a patch

Oracle has released patches that address some of these vulnerabilities. Patch information can be found in [Oracle Security Alert #28](#) and [Oracle Security Alert #25](#) and on the [MetaLink](#) web site (registration required).

Secure default configuration

Oracle has provided documentation on changing vulnerable default configuration settings. For details, consult individual Vulnerability Notes and the Oracle Security Alerts referenced [above](#).

The CERT Coordination Center thanks David Litchfield and Oracle for information used in this document.

Authors: [Art Manion](#), [Jason A. Rafail](#), and [Shawn Van Ittersum](#)

Appendix A Vendor Information

This appendix contains statements provided by vendors for this advisory. We will update this section as vendors provide new or modified statements, and we will note the changes in our revision history. If a particular vendor is not listed below, we have not received their comments.

Appendix B References

1. <http://www.kb.cert.org/vuls/id/500203>
2. <http://www.kb.cert.org/vuls/id/313280>
3. <http://www.kb.cert.org/vuls/id/750299>
4. <http://www.kb.cert.org/vuls/id/878603>
5. <http://www.kb.cert.org/vuls/id/659043>
6. <http://www.kb.cert.org/vuls/id/923395>
7. <http://www.kb.cert.org/vuls/id/307835>
8. <http://www.kb.cert.org/vuls/id/736923>
9. <http://www.kb.cert.org/vuls/id/611776>
10. <http://www.kb.cert.org/vuls/id/698467>
11. <http://www.kb.cert.org/vuls/id/476619>
12. <http://www.kb.cert.org/vuls/id/712723>
13. <http://www.kb.cert.org/vuls/id/168795>

14. <http://www.kb.cert.org/vuls/id/278971>
15. <http://www.kb.cert.org/vuls/id/180147>
16. <http://www.kb.cert.org/vuls/id/193523>
17. <http://www.kb.cert.org/vuls/id/977251>
18. <http://www.kb.cert.org/vuls/id/805915>
19. <http://www.kb.cert.org/vuls/id/547459>
20. <http://www.nextgenss.com/papers/hpoas.pdf>
21. <http://www.nextgenss.com/advisories/plsql.txt>
22. <http://www.nextgenss.com/advisories/oraplsxtproc.txt>
23. <http://www.nextgenss.com/advisories/oraplsbos.txt>
24. <http://www.nextgenss.com/advisories/orajsa.txt>
25. <http://www.nextgenss.com/advisories/orajsp.txt>
26. http://otn.oracle.com/deploy/security/pdf/plsxtproc_alert.pdf
27. http://otn.oracle.com/deploy/security/pdf/ias_modplsql_alert.pdf
28. <http://otn.oracle.com/deploy/security/pdf/modplsql.pdf>
29. http://otn.oracle.com/deploy/security/pdf/ias_soap_alert.pdf

Copyright 2002 Carnegie Mellon University

Revision History

March 14, 2002: Initial release

March 14, 2002: Changed title and references to Appendix A.

March 15, 2002: Added Oracle Database language to Description section

September 17, 2002: Fixed Oracle search URL

9 CA-2002-09: Multiple Vulnerabilities in Microsoft IIS

Original release date: April 11, 2002

Last revised: --

Source: CERT/CC

A complete revision history can be found at the end of this file.

Systems Affected

- Microsoft IIS 4.0, 5.0, and 5.1

Overview

A variety of vulnerabilities exist in various versions of Microsoft IIS. Some of these vulnerabilities may allow an intruder to execute arbitrary code on vulnerable systems.

I. Description

There are a variety of vulnerabilities in Microsoft IIS. Many of these vulnerabilities are buffer overflows that could permit an intruder to execute arbitrary code on vulnerable systems.

We strongly encourage all sites running IIS to read Microsoft's advisory on these and other vulnerabilities and take appropriate action as soon as practical. Microsoft's bulletin is available at

<http://www.microsoft.com/technet/security/bulletin/MS02-018.asp>

Additional information about these vulnerabilities is available at

Vulnerability note	<u>CVE</u> num- ber	Title
http://www.kb.cert.org/vuls/id/363715	<u>CAN-</u> <u>2002-</u> <u>0071</u>	Microsoft Internet Information Server (IIS) vulnerable to heap overflow during processing of crafted ".htr" request by "ISM.DLL" ISAPI filter

http://www.kb.cert.org/vuls/id/883091	<u>CAN-2002-0074</u>	Microsoft Internet Information Server (IIS) contains cross-site scripting vulnerability in IIS Help Files search facility
http://www.kb.cert.org/vuls/id/886699	<u>CAN-2002-0148</u>	Microsoft Internet Information Server (IIS) contains cross-site scripting vulnerability in HTTP error page results
http://www.kb.cert.org/vuls/id/520707	<u>CAN-2002-0075</u>	Microsoft Internet Information Server (IIS) contains cross-site scripting vulnerability in redirect response messages
http://www.kb.cert.org/vuls/id/412203	<u>CAN-2002-0073</u>	Microsoft Internet Information Server (IIS) vulnerable to DoS via malformed FTP connection status request
http://www.kb.cert.org/vuls/id/454091	<u>CAN-2002-0150</u>	Microsoft Internet Information Server (IIS) vulnerable to buffer overflow via inaccurate checking of delimiters in HTTP header fields
http://www.kb.cert.org/vuls/id/721963	<u>CAN-2002-0149</u>	Microsoft Internet Information Server (IIS) buffer overflow in server-side includes (SSI) containing long invalid file name
http://www.kb.cert.org/vuls/id/521059	<u>CAN-2002-0072</u>	Microsoft Internet Information Server (IIS) vulnerable to DoS when URL request exceeds maximum allowed length

http://www.kb.cert.org/vuls/id/610291	<u>CAN-2002-0079</u>	Microsoft Internet Information Server (IIS) buffer overflow in chunked encoding transfer mechanism
http://www.kb.cert.org/vuls/id/669779	<u>CAN-2002-0147</u>	Microsoft Internet Information Server (IIS) buffer overflow in chunked encoding transfer mechanism

II. Impact

For many of the vulnerabilities, an intruder could execute arbitrary code with privileges that vary according to which version of IIS is running. In general, IIS 4.0 permits an intruder to execute code with complete administrative privileges, while IIS 5.0 and 5.1 permit an intruder to execute code with the privileges of the IWAM_computername account.

III. Solution

Microsoft Corporation has released Microsoft Security Bulletin MS02-018, which announces the availability of a cumulative patch to address a variety of problems. We strongly encourage you to read this bulletin and take the appropriate corrective measures. MS02-018 is available at

<http://www.microsoft.com/technet/security/bulletin/MS02-018.asp>

In addition to applying the patch, or until it can be applied, we recommend the following actions:

- Use the IIS Lockdown tool and URLScan to eliminate or reduce the impact of some of these vulnerabilities; they may also eliminate or reduce other vulnerabilities that have not yet been discovered. The IIS Lockdown tool can also be used to disable ASP if it's not needed. More information about the IIS Lockdown tool and URLScan can be found at

<http://www.microsoft.com/technet/security/tools/locktool.asp>

<http://www.microsoft.com/technet/security/URLScan.asp>

- As Microsoft has recommended for quite some time, disable the HTR ISAPI extension unless it is absolutely required.
- Disable anonymous FTP unless it is required.
- Don't give login credentials on IIS servers to untrusted users.

Our thanks to Microsoft Corporation for the information contained in their advisory. Additionally, our thanks go to the various individuals and organizations whom Microsoft identified as discovering the vulnerabilities, including eEye Digital Security (<http://www.eeye.com>), Serge Mister of Entrust, Inc. (<http://www.entrust.com>), Dave Aitel of @Stake (<http://www.atstake.com>), Peter Grundl of KPMG, Joe Smith (jsm1th@hotmail.com) and zenomorph (admin@cgisecurity.com) of <http://www.cgisecurity.com>, Keigo Yamazaki of the LAC SNS Team (<http://www.lac.co.jp/security/>), and Thor Larholm of Jubii A/S.

Author: Shawn V. Hernan

Copyright 2002 Carnegie Mellon University

Revision History

April 11, 2002: Initial release

10 CA-2002-10: Format String Vulnerability in rpc.rwalld

Original release date: May 1, 2002

Last revised: May 15, 2002

Source: CERT/CC

A complete revision history can be found at the end of this file.

Systems Affected

- Sun Solaris 2.5.1, 2.6, 7, and 8

Overview

The rwall daemon (rpc.rwalld) is a utility that is used to listen for wall requests on the network. When a request is received, it calls wall, which sends the message to all terminals of a time-sharing system. A format string vulnerability may permit an intruder to execute code with the privileges of the rwall daemon. A proof of concept exploit is publicly available, but we have not seen active scanning or exploitation of this vulnerability.

I. Description

rpc.rwalld is a utility that listens for remote wall requests. Wall is used to send a message to all terminals of a time-sharing system. If the wall command cannot be executed, the rwall daemon will display an error message.

An intruder can consume system resources and potentially prevent wall from executing, which would trigger the rwall daemon's error message. A format string vulnerability exists in the code that displays the error message. This vulnerability may permit the intruder to execute code with the privileges of the rwall daemon.

This vulnerability may be exploited both locally and remotely, although remote exploitation is significantly more difficult.

II. Impact

An intruder can execute code with the privileges of the rwall daemon, typically root.

III. Solution

Apply a patch

[Appendix A](#) contains information provided by vendors for this advisory.

If a patch is not available, disable the rwall daemon (rpc.rwalld) in inetd.conf until a patch can be applied.

If disabling the rwall daemon is not an option, implement a firewall to limit access to rpc.rwalld (typically port 32777/UDP). Note that this will not mitigate all vectors of attack.

Appendix A Vendor Information

This appendix contains information provided by vendors for this advisory. As vendors report new information to the CERT/CC, we will update this section and note the changes in our revision history. If a particular vendor is not listed below, please check the [Vulnerability Note \(VU#638099\)](#) or contact your vendor directly.

Apple

Mac OS X does not contain rwall, and is not susceptible to the vulnerability described.

BSDI

BSD/OS does not include an affected daemon in any version.

Compaq Computer Corporation

Compaq Tru64 is NOT vulnerable to this reported problem.

Cray, Inc.

Cray, Inc. is not vulnerable since the affected code is not included in the rwalld implementation used in Unicos and Unicos/mk.

FreeBSD

FreeBSD is not vulnerable to this problem.

Hewlett-Packard

HP is not vulnerable.

IBM

IBM's AIX operating system, versions 4.3.x and 5.1L, is not susceptible to the vulnerability described.

NEC

sent on May 15, 2002

[Server Products]

- EWS/UP 48 Series
 - is NOT vulnerable.

NetBSD

NetBSD has never been vulnerable to this problem.

Sun Microsystems

Sun confirms that there is a format string vulnerability in rpc.rwalld(1M) which affects Solaris 2.5.1, 2.6, 7 and 8. However, this issue relies on a combination of events, including the exhaustion of system resources, which are difficult to control by a remote user in order to be exploited. Disabling rpc.rwalld(1M) in inetd.conf(4) is the recommended workaround until patches are available.

Sun is currently generating patches for this issue and will be releasing a Sun Security Bulletin once the patches are available. The bulletin will be available from <http://sunsolve.sun.com/security>.

Sun patches are available from <http://sunsolve.sun.com/securitypatch>.

The CERT Coordination Center acknowledges "GOBBLES" as the discoverer of this vulnerability and thanks Sun Microsystems for their technical information.

Feedback can be directed to the author: [Jason A. Rafail](#)

Copyright 2002 Carnegie Mellon University

Revision History

May 1, 2002: Initial release
May 2, 2002: Added Apple vendor statment.
May 2, 2002: Added Compaq vendor statment.
May 2, 2002: Added Cray vendor statment.
May 2, 2002: Added FreeBSD vendor statment.
May 2, 2002: Added BSDI vendor statment.
May 15, 2002: Added NEC vendor statment.

11 CA-2002-11: Heap Overflow in Cachefs Daemon (cachefsd)

Original release date: May 06, 2002

Last revised: May 14, 2002

Source: CERT/CC

A complete revision history can be found at the end of this file.

Systems Affected

- Sun Solaris 2.5.1, 2.6, 7, and 8 (SPARC and Intel architectures)

Overview

Sun's NFS/RPC file system cachefs daemon (cachefsd) is shipped and installed by default with Sun Solaris 2.5.1, 2.6, 7, and 8 (SPARC and Intel architectures). A remotely exploitable vulnerability exists in cachefsd that could permit a remote attacker to execute arbitrary code with the privileges of the cachefsd, typically root. The CERT/CC has received credible reports of scanning and exploitation of Solaris systems running cachefsd.

I. Description

A remotely exploitable heap overflow exists in the cachefsd program shipped and installed by default with Sun Solaris 2.5.1, 2.6, 7, and 8 (SPARC and Intel architectures). Cachefsd caches requests for operations on remote file systems mounted via the use of NFS protocol. A remote attacker can send a crafted RPC request to the cachefsd program to exploit the vulnerability.

Logs of exploitation attempts may resemble the following:

```
May 16 22:46:08 victim-host inetd[600]:  
/usr/lib/fs/cachefs/cachefsd: Segmentation Fault - core dumped
```

```
May 16 22:46:21 victim-host last message repeated 7 times
```

```
May 16 22:46:22 victim-host inetd[600]:  
/usr/lib/fs/cachefs/cachefsd: Bus Error - core dumped
```

```
May 16 22:46:24 victim-host inetd[600]:  
/usr/lib/fs/cachefs/cachefsd: Segmentation Fault - core dumped
```

```
May 16 22:46:56 victim-host inetd[600]:  
/usr/lib/fs/cachefs/cachefsd: Bus Error - core dumped
```

```
May 16 22:46:59 victim-host last message repeated 1 time
```

```
May 16 22:47:02 victim-host inetd[600]:  
/usr/lib/fs/cachefs/cachefsd: Segmentation Fault - core dumped
```

```
May 16 22:47:07 victim-host last message repeated 3 times
```

```
May 16 22:47:09 victim-host inetd[600]:  
/usr/lib/fs/cachefs/cachefsd: Hangup
```

```
May 16 22:47:11 victim-host inetd[600]:  
/usr/lib/fs/cachefs/cachefsd: Segmentation Fault - core dumped
```

Sun Microsystems has released a [Sun Alert Notification](#) which addresses this issue as well as the issue described in [VU#161931](#).

According to the [Sun Alert Notification](#), failed attempts to exploit this vulnerability may leave a core dump file in the root directory. The presence of the *core* file does not preclude the success of subsequent attacks. Additionally, if the file */etc/cachefstab* exists, it may contain unusual entries.

This issue is also being referenced as [CAN-2002-0033](#):

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0033>

II. Impact

A remote attacker may be able to execute code with the privileges of the cachefsd process, typically root.

III. Solution

Apply a patch from your vendor

[Appendix A](#) contains information provided by vendors for this advisory.

If a patch is not available, disable cachefsd in *inetd.conf* until a patch can be applied.

If disabling the cachefsd is not an option, follow the suggested workaround in the [Sun Alert Notification](#).

Appendix A Vendor Information

This appendix contains information provided by vendors for this advisory. As vendors report new information to the CERT/CC, we will update this section and note the changes in our revision history. If a particular vendor is not listed below, please check the [Vulnerability Note \(VU#635811\)](#) or contact your vendor directly.

Cray, Inc.

Cray, Inc. is not vulnerable since cachefs is not supported under Unicos and Unicos/mk.

Fujitsu

UXP/V is not vulnerable, because it does not have Cachefs and similar functionalities.

Hewlett-Packard

HP-UX is not vulnerable because it does not use cachefsd.

IBM

IBM's AIX operating system, all versions, is not vulnerable.

Nortel Networks

Nortel Networks products and solutions using the affected Sun Solaris operating systems do not utilize the NFS/RPC file system cachefs daemon. Nortel Networks recommends following the mitigating practices in Sun Microsystems Inc.'s Alert Notification.; this will not impact these Nortel Networks products and solutions.

For more information please contact Nortel at:

North America: 1-8004NORTEL or 1-800-466-7835

Europe, Middle East and Africa: 00800 8008 9009, or +44 (0) 870 907 9009

Contacts for other regions are available at

www.nortelnetworks.com/help/contact/global/

SGI

SGI does not ship with SUN cachefsd, so IRIX is not vulnerable.

Sun

See the Sun Alert Notification available at <http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F44309>.

The CERT/CC acknowledges the Last Stage of Delirium Team for discovering and reporting on this vulnerability and thanks Sun Microsystems for their technical assistance.

Feedback can be directed to the authors: [Jason A. Rafail and Jeffrey S. Havrilla](#)

Copyright 2002 Carnegie Mellon University

Revision History

May 06, 2002: Initial release

May 06, 2002: Corrected CVE number and links

May 07, 2002: Added Hewlett-Packard vendor statement

May 07, 2002: Corrected credit statement

May 09, 2002: Corrected credit statement

May 09, 2002: Corrected CVE number and links

May 09, 2002: Removed AusCERT Advisory

11: CA-2002-11: Heap Overflow in Cachefs Daemon (cachefsd)

May 13, 2002: Added Cray vendor statement

May 13, 2002: Added Nortel Networks vendor statement

May 14, 2002: Added Fujitsu vendor statement

12 CA-2002-12: Format String Vulnerability in ISC DHCPD

Original release date: May 8, 2002

Last revised: Mon Oct 7 09:10:52 EDT 2002

Source: CERT/CC

A complete revision history can be found at the end of this file.

Systems Affected

- ISC DHCPD 3.0 to 3.0.1rc8 inclusive

Overview

The Internet Software Consortium (ISC) provides a Dynamic Host Configuration Protocol Daemon (DHCPD), which is a server that is used to allocate network addresses and assign configuration parameters to hosts. A format string vulnerability may permit a remote attacker to execute code with the privileges of the DHCPD (typically root). We have not seen active scanning or exploitation of this vulnerability.

I. Description

ISC's DHCPD listens for requests from client machines connecting to the network. Versions 3 to 3.0.1rc8 (inclusive) of DHCPD contains an option (NSUPDATE) that is enabled by default. NSUPDATE allows the DHCP server to send information about the host to the DNS server after processing a DHCP request. The DNS server responds by sending an acknowledgement message back to the DHCP server that may contain user-supplied data (like a host name). When the DHCP server receives the acknowledgement message from the DNS server, it logs the transaction.

A format string vulnerability exists in ISC's DHCPD code that logs the transaction. This vulnerability may permit a remote attacker to execute code with the privileges of the DHCP daemon.

II. Impact

A remote attacker may be able to execute code with the privileges of the DHCPD (typically root).

III. Solution

Note that some of the mitigation steps recommended below may have significant impact on your normal network operations. Ensure that any changes made based on the following recommendations will not unacceptably affect any of your operations.

Apply a patch from your vendor

Appendix A contains information provided by vendors for this advisory.

Disable the DHCP service

As a general rule, the CERT/CC recommends disabling any service or capability that is not explicitly required. Depending on your network configuration, you may not need to use DHCP.

Ingress filtering

As a temporary measure, it may be possible to limit the scope of this vulnerability by blocking access to DHCP services at the network perimeter.

Ingress filtering manages the flow of traffic as it enters a network under your administrative control. In the network usage policy of many sites, there are few reasons for external hosts to initiate inbound traffic to machines that provide no public services. Thus, ingress filtering should be performed at the border to prohibit externally initiated inbound traffic to non-authorized services. For DHCP, ingress filtering of the following ports can prevent attackers outside of your network from reaching vulnerable devices in the local network that are not explicitly authorized to provide public DHCP services.

```
bootps 67/tcp # Bootstrap Protocol Server
bootps 67/udp # Bootstrap Protocol Server
bootpc 68/tcp # Bootstrap Protocol Client
bootpc 68/udp # Bootstrap Protocol Client
```

Appendix A Vendor Information

This appendix contains information provided by vendors for this advisory. As vendors report new information to the CERT/CC, we will update this section and note the changes in our revision history. If a particular vendor is not listed below, please check the Vulnerability Note (VU#854315) or contact your vendor directly.

Alcatel

Following the recent CERT advisory on security vulnerabilities in the ISC DHCP implementation, Alcatel has conducted an immediate assessment to determine any impact this may have on our portfolio. A first analysis has shown that only one customer-specific product was affected. Alcatel is working with that customer on a solution. The security of our customers' networks is of highest priority for Alcatel. Therefore we continue to test our product portfolio against potential ISC DHCP security vulnerabilities and will provide updates if necessary.

Apple Computer, Inc.

Mac OS X does not contain this vulnerability.

Conectiva

Please see the [Conectiva Linux Announcement](#).

Cray Inc.

Cray, Inc. is not vulnerable since dhcp is not supported under Unicos or Unicos/mk.

F5 Networks, Inc.

F5 Networks' products do not include any affected version of ISC's DHCPD, and are therefore not vulnerable.

FreeBSD

The FreeBSD base system does not ship with the ISC dhcpd server by default and is not affected by this vulnerability. The ISC dhcpd server is available in the FreeBSD Ports Collection; updates to the ISC dhcp port (ports/net/isc-dhcp3) are in progress and corrected packages will be available in the near future.

Fujitsu Limited

Fujitsu's UXP/V operating system is not vulnerable. UXP/V does not support dhcp.

Hewlett-Packard Company

HP-UX is not vulnerable.

IBM

IBM's AIX operating system, all versions, is not vulnerable.

Internet Software Consortium

A patch is included below, and we have a patched version of 3.0 available (3.0p11) and a new release candidate for the next bug-fix release (3.0.1RC9). Both of these new releases are not vulnerable.

```
--- common/print.c Tue Apr 9 13:41:17 2002
+++ common/print.c.patched Tue Apr 9 13:41:56 2002
@@ -1366,8 +1366,8 @@
 *s++ = '!';
 *s++ = 0;
 if (errorp)
 - log_error (obuf);
 + log_error ("%s",obuf);
 else
```

```
- log_info (obuf);  
+ log_info ("%s",obuf);  
}  
#endif /* NSUPDATE */
```

Lotus Development Corporation

This issue does not affect Lotus products.

Microsoft Corporation

Microsoft does not ship the ISC DHCPD program.

NEC Corporation

EWS/UP 48 Series is NOT vulnerable.

NetBSD

NetBSD fixed this during a format string sweep performed on 11-Oct-2000. No released version of NetBSD is vulnerable to this issue.

Nortel Networks Limited

Nortel Networks products are not impacted by this vulnerability.

Novell

Novell does not ship ISC's DHCPD.

Red Hat

Red Hat Linux has never been shipped with version 3 of dhcpd and therefore none of our releases are vulnerable to this issue.

Silicon Graphics, Inc.

SGI is not vulnerable.

Sun Microsystems

Sun is not vulnerable as Solaris does not ship the ISC DHCPD and does not use any of the ISC DHCPD source in its version of DHCPD.

Xerox

Xerox is aware of this advisory. A response is available from our web site:
<http://www.xerox.com/security> .

The CERT Coordination Center acknowledges Next Generation Security Technologies as the discoverer of this vulnerability and thanks them and the Internet Software Consortium (ISC) for their cooperation, reporting, and analysis of this vulnerability.

Feedback can be directed to the author: Ian A. Finlay.

Copyright 2002 Carnegie Mellon University

Revision History

May 08, 2002: Initial release
May 09, 2002: Added vendor statement for Nortel Networks Limited
May 10, 2002: Revised vendor statement for Conectiva
May 13, 2002: Added vendor statement for Cray Inc.
May 14, 2002: Added vendor statement for Fujitsu Limited
May 14, 2002: Added vendor statement for Apple Computer, Inc.
May 14, 2002: Added vendor statement for NEC Corporation
May 23, 2002: Added vendor statement for Novell
May 29, 2002: Revised vendor statement for Alcatel
May 31, 2002: Added vendor statement for Sun Microsystems
Jun 11, 2002: Added vendor statement for Red Hat, Inc.
Aug 21, 2002: Added vendor statement for Xerox
Oct 07, 2002: Fixed link for Xerox

13 CA-2002-13: Buffer Overflow in Microsoft's MSN Chat ActiveX Control

Original release date: May 10, 2002

Last revised: August 28, 2002

Source: CERT/CC

A complete revision history can be found at the end of this file.

Systems Affected

Microsoft Windows systems with one or more of the following:

- Microsoft MSN Chat control
- Microsoft MSN Messenger 4.6 and prior
- Microsoft Exchange Instant Messenger 4.6 and prior

Overview

Microsoft's MSN Chat is an ActiveX control for Microsoft Messenger, an instant messaging client. A buffer overflow exists in the ActiveX control that may permit a remote attacker to execute arbitrary code on the system with the privileges of the current user.

I. Description

A buffer overflow exists in the "ResDLL" parameter of the MSN Chat ActiveX control that may permit a remote attacker to execute arbitrary code on the system with the privileges of the current user. This vulnerability affects MSN Messenger and Exchange Instant Messenger users. Since the control is signed by Microsoft, users of Microsoft's Internet Explorer (IE) who accept and install Microsoft-signed ActiveX controls are also affected. The Microsoft MSN Chat control is also available for direct download from the web.

The <object> tag could be used to embed the ActiveX control in a web page. If an attacker can trick the user into visiting a malicious site or the attacker sends the victim a web page as an HTML-formatted email message or newsgroup posting then this vulnerability could be exploited. This acceptance and installation of the control can occur automatically within IE for users who trust Microsoft-signed ActiveX controls. When the web page is rendered, either by opening the page or viewing the page through a preview pane, the ActiveX control could be invoked. Likewise, if the ActiveX control is embedded in a Microsoft Office (Word, Excel, etc.) document, it may be executed when the document is opened.

According to the [Microsoft Advisory \(MS02-022\)](#):

It's important to note that this control is used for chat rooms on several MSN sites in addition to the main MSN Chat site. If you have successfully used chat on any MSN-site, you have downloaded and installed the chat control.

The CERT/CC has published information on ActiveX in *Results of the Security in ActiveX Workshop* (pdf) and [CA-2000-07](#).

This issue is also being referenced as [CAN-2002-0155](#):
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0155>.

II. Impact

A remote attacker may be able to execute arbitrary code with the privileges of the current user.

III. Solution

Apply a patch from your vendor

On June 11, 2002, Microsoft updated Microsoft Advisory (MS02-022) and released a new patch that remedies the vulnerability for users that downloaded and accepted the control. The previous solution did not fully protect against this action and it was possible for an attacker to load the vulnerable control, even though the previous patch and updated versions had been installed.

The new patch is available at <http://www.microsoft.com/Downloads/Release.asp?ReleaseID=39632>. All users should apply this patch, even if you previously installed an updated version of your software. This patch supercedes the patch information below.

Microsoft has released a patch, a fixed MSN Chat control, and upgrades to address this issue. It is important that all users apply the patch since it will prevent the installation of the vulnerable control on systems that have not already installed it.

Download location for the patch:

<http://www.microsoft.com/Downloads/Release.asp?ReleaseID=38790>

If you have updated your software prior to June 11, 2002, you should reinstall the software from the following locations:

Download location for updated version of MSN Messenger with the corrected control:

<http://messenger.msn.com/download/download.asp?client=1&update=1>

Download location for updated version of Exchange Instant Messenger with the corrected control:

<http://www.microsoft.com/Exchange/downloads/2000/IMclient.asp>

Microsoft also suggests that the following Microsoft mail products: Outlook 98 and Outlook 2000 with the [Outlook Email Security Update](#), Outlook 2002, and Outlook Express will block the exploitation of this vulnerability via email because these products will open HTML email in the Restricted Sites zone.

Other mitigation strategies include opening web pages and email messages in the Restricted Sites zone and using email clients that permit users to view messages in plain-text. Likewise, it is important for users to realize that a signed control only authenticates the origin of the control and does not imply any information with regard to the security of the control. Therefore, downloading and installing signed controls through an automated process is not a secure choice.

Appendix A Vendor Information

This appendix contains information provided by vendors for this advisory. As vendors report new information to the CERT/CC, we will update this section and note the changes in our revision history. If a particular vendor is not listed below, please check the [Vulnerability Note \(VU#713779\)](#) or contact your vendor directly.

Microsoft

See <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-022.asp>

The CERT/CC acknowledges the eEye Team for discovering and reporting on this vulnerability and thanks Microsoft for their technical assistance.

Feedback can be directed to the author: [Jason A. Rafail](#).

Copyright 2002 Carnegie Mellon University

Revision History

May 10, 2002: Initial release

August 28, 2002: Updated patch information

14 CA-2002-14: Buffer overflow in Macromedia JRun

Original release date: May 29, 2002

Last revised: Wed Aug 21 14:00:33 EDT 2002

Source: CERT/CC

A complete revision history can be found at the end of this file.

Systems Affected

- Windows NT4 or Windows 2000 running IIS versions 4 or 5 and Macromedia JRun 3.0 or 3.1

Overview

A remotely exploitable buffer overflow exists in Macromedia's JRun 3.0 and 3.1.

I. Description

JRun is an application server that works with most popular web servers, such as Apache and Internet Information Server (IIS). According to Macromedia, JRun is deployed at over 10,000 organizations worldwide.

As reported in the Next Generation Security Software Advisory (#NISR29052002), a remotely exploitable buffer overflow exists in the ISAPI filter/application. Specifically, the buffer overflow exists in the portion of code that handles the host header field. If an attacker sends a specially crafted request to the application server, he can overwrite a return address on the stack. Because the vulnerable DLL is running in the address space of the web server process, code submitted by the attacker will be run with SYSTEM privileges.

II. Impact

A remote attacker can execute arbitrary code on the vulnerable target with SYSTEM privileges.

III. Solution

Apply a patch from Macromedia or upgrade to JRun 4.

Appendix A Vendor Information

This appendix contains information provided by vendors for this advisory. Additional information can be found at VU#703835.

Macromedia Inc.

Macromedia has confirmed that this is a problem in older versions of JRun 3.0 and 3.1 and is soon to publish a security bulletin regarding this. Visit the Macromedia security zone site at <http://www.macromedia.com/security> for more information.

This vulnerability was discovered by David Litchfield of Next Generation Security Software.

Author: Ian A. Finlay

Copyright 2002 Carnegie Mellon University

Revision History

May 29, 2002: Initial release

Aug 21, 2002: Fixed Macromedia link

15 CA-2002-15: Denial-of-Service Vulnerability in ISC BIND 9

Original release date: June 04, 2002

Last revised: Wed Sep 18 10:40:08 EDT 2002

Source: CERT/CC

A complete revision history can be found at the end of this file.

Systems Affected

- Domain Name System (DNS) servers running ISC BIND 9 prior to 9.2.1
Because the normal operation of most services on the Internet depends on the proper operation of DNS servers, other services could be affected if this vulnerability is exploited.

Overview

A denial-of-service vulnerability exists in version 9 of the Internet Software Consortium's (ISC) Berkeley Internet Name Domain (BIND) server. ISC BIND versions 8 and 4 are not affected. Exploiting this vulnerability will cause the BIND server to shut down.

I. Description

BIND is an implementation of the Domain Name System (DNS) that is maintained by the ISC. A vulnerability exists in version 9 of BIND that allows remote attackers to shut down BIND servers. An attacker can cause the shutdown by sending a specific DNS packet designed to trigger an internal consistency check. However, this vulnerability will not allow an attacker to execute arbitrary code or write data to arbitrary locations in memory.

The internal consistency check that triggers the shutdown occurs when the `rdataset` parameter to the `dns_message_findtype()` function in `message.c` is not NULL as expected. The condition causes the code to assert an error message and call `abort()` to shut down the BIND server. It is also possible to accidentally trigger this vulnerability using common queries found in routine operation, especially queries originating from SMTP servers.

A vulnerability note describing this problem can be found at <http://www.kb.cert.org/vuls/id/739123>. This vulnerability note includes a list of vendors that have been contacted about this vulnerability.

This vulnerability is also being referenced as [CAN-2002-0400](#):
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0400>

II. Impact

Exploitation of this vulnerability will cause the BIND server to abort and shut down. As a result, the BIND server will not be available unless it is restarted.

III. Solution

Apply a patch from your vendor

The ISC has released BIND version 9.2.1. The CERT/CC recommends that users of BIND 9 apply a patch from their vendor or upgrade to [BIND 9.2.1](#).

Appendix A Vendor Information

This appendix contains information provided by vendors for this advisory. As vendors report new information to the CERT/CC, we will update this section and note the changes in our revision history. If a particular vendor is not listed below, we have not received their comments.

Alcatel

In relation to this CERT advisory on security vulnerabilities with ISC BIND 9 implementation, Alcatel has conducted an immediate assessment to determine any impact this may have on our portfolio. An initial analysis has shown that none of our products is affected when used as delivered to customers. The security of our customers' networks is of highest priority for Alcatel. Therefore, investigations are going on, in particular for the UMTS GPRS Core Network portfolio, to determine any impact. Updates will be provided if necessary. Customers may contact their Alcatel support representative for more details.

Apple

The version of BIND that ships in Mac OS X and Mac OS X Server does not contain this vulnerability.

BSDI

Wind River Systems, Inc. does not include BIND 9 with any version of BSD/OS.

Caldera

SCO OpenServer from Caldera does not ship BIND9, and is therefore not vulnerable.

Caldera Open UNIX does ship BIND9, and is vulnerable. We are investigating.

Caldera OpenLinux does not ship BIND9, and is therefore not vulnerable.

Compaq Computer Corporation

HP Alpha Server Products:

HP Tru64 UNIX:

Tru64 UNIX is not vulnerable to this reported problem. HP Tru64 UNIX ships with BIND 8.2.2-p5

TCP/IP for HP OpenVms:

TCP/IP for HP OpenVms is not vulnerable to this reported problem. The current versions of TCP/IP for HP OpenVMS ship BIND 8.2.2-p5

HP NonStop Server:

"HP NonStop Himalaya is not vulnerable to this problem. The 'named' function of Domain Name Server (T6021) which is implemented for HP NonStop Himalaya is based on BIND 4.8. NonStop DNS is the only Himalaya software product that includes 'named'."

Cray

Cray, Inc. is not vulnerable since the BIND distributed with Unicos and Unicos/mk is not based on BIND 9.

djbdns

djbdns does not have this bug. Unlike BIND 9, djbdns does not commit hara-kiri when an attacker tries to confuse it, or pokes it sharply, or simply thinks bad thoughts in its general direction. djbdns has never used any BIND-derived code. See <http://cr.yp.to/djbdns.html> .

Engarde

Guardian Digital does not ship BIND 9 in any versions of EnGarde Secure Linux, therefore we are not vulnerable. All versions were shipped with BIND 8.

F5 Networks, Inc.

EDGE-FX contains a vulnerable version of BIND 9. Instructions for obtaining and installing a patch are available at ftp://ftp.f5.com/Domestic/Edgefx/named_patch/cert_patch_6_2002.html.

All other F5 Networks products contain BIND 8.2, and are therefore not affected by this vulnerability.

FreeBSD

The FreeBSD base system does not ship with ISC BIND 9. However, ISC BIND 9 is available in the FreeBSD Ports Collection. It is currently at version 9.2.1 and is therefore unaffected.

Hewlett-Packard Company

HEWLETT-PACKARD COMPANY SECURITY BULLETIN: HPSBUX0207-202

Originally issued: 22 July 2002

HP Published Security Bulletin HPSBUX0207-202 with solutions for HP9000 Series 700/800 running HP-UX release 11.11 (11i) only with the BINDv920.INETSVCS-BIND fileset installed.

This bulletin is available from the HP IT Resource Center page at: <http://itrc.hp.com> "Maintenance and Support" then "Support Information Digests" and then "hp security bulletins archive" search for bulletin HPSBUX0207-202.

IBM

After analysis of the affected component, IBM has determined that the AIX bind daemon is not vulnerable to the attack as described in the CERT advisory.

Inktomi Corporation

Inktomi Inktomi Traffic Server DNS proxy does not include BIND9 and is therefore not vulnerable.

Internet Software Consortium

This vulnerability was found through routine bug analysis. BIND 9 is designed to exit when it detects an internal consistency error to reduce the impact of bugs in the server. ISC strongly recommends that all BIND 9 users upgrade immediately to 9.2.1. BIND 9.2.1 can be found at <http://www.isc.org/products/BIND/bind9.html>.

MandrakeSoft

Mandrake Linux 8.x ships with BIND9 and as such updated packages will be available as early as possible.

Microsoft Corporation

Microsoft has reviewed the information and can confirm that our products are not affected by this vulnerability.

NEC Corporation

sent on June 3, 2002

[Server Products]

* EWS/UP 48 Series operating system
- is NOT vulnerable.

NetBSD

NetBSD has not included Bind 9 in the base system of any release or -current development branch.

Bind 9 is available from the 3rd party software system, pkgsrc. Users who have installed net/bind9 or net/bind9-current should update to a fixed version. pkgsrc/security/audit-packages can be used to keep up to date with these types of issues.

Network Appliance

All NetApp products do not contain any BIND code, so no NetApp product is vulnerable to this problem.

Nortel Networks Limited

Nortel Networks is reviewing its portfolio to determine if any products are affected by the vulnerability noted in CERT Advisory CA-2002-15. A definitive statement will be issued shortly.

Red Hat

Red Hat distributed BIND 9 in Red Hat Linux versions 7.1, 7.2, and 7.3. We are currently working on producing errata packages, when complete these will be available along with our advisory at the URL below. At the same time users of the Red Hat Network will be able to update their systems using the 'up2date' tool.

<http://rhn.redhat.com/errata/RHSA-2002-105.html>

Silicon Graphics, Inc.

IRIX does not ship with BIND9 and is not vulnerable.

Sun Microsystems

Sun does not ship BIND 9 with any version of Solaris at this time and is therefore not affected by this issue.

SuSE, Inc.

We are affected by the bind9 DoS issue as well. All of our currently supported SuSE Linux products come with a bind9 package. We will release an announcement for the issue, coordinated with your timeframe and not before we see your official announcement.

Unisphere Networks, Inc.

The Unisphere Networks ERX family of edge routers does not implement a DNS server or named daemon within the Unison OS. Additionally, the DNS client found on the ERX is not based on the

ISC BIND code. Unisphere Networks has no reason to expect a similar problem exists in the DNS client implementation found on the ERX.

The CERT Coordination Center thanks the Internet Software Consortium for notifying us about this vulnerability.

Author: Ian A. Finlay

Copyright 2002 Carnegie Mellon University

Revision History

June 04, 2002: Initial release

June 11, 2002: Added vendor statement for djbdns

June 11, 2002: Added vendor statement for Inktomi Corporation

June 11, 2002: Updated vendor statement for F5 Networks, Inc.

Aug 08, 2002: Added vendor statement for Hewlett Packard

Sep 18, 2002: Added vendor statement for Alcatel

16 CA-2002-16: Multiple Vulnerabilities in Yahoo! Messenger

Original release date: June 05, 2002

Last revised: June 07, 2002

Source: CERT/CC

A complete revision history can be found at the end of this file.

Systems Affected

U.S. and International versions of:

- Yahoo! Messenger version 5,0,0,1064 and prior for Microsoft Windows

Overview

There are multiple vulnerabilities in Yahoo! Messenger. Attackers that are able to exploit these vulnerabilities may be able to execute arbitrary code with the privileges of the victim user. We have not seen active scanning for these vulnerabilities, nor have we received any reports of these vulnerabilities being exploited, but users should upgrade to the version 5,0,0,1065 or later.

I. Description

Yahoo! Messenger is a widely used program for communicating with other users over the Internet. On May 27, 2002, a buffer overflow and a URL validation vulnerability were discovered in the Yahoo! Messenger client for Microsoft Windows. Details of each vulnerability follow:

VU#137115 - Yahoo! Messenger contains a buffer overflow in the URI handler

The buffer overflow occurs during the processing of the Yahoo! Messenger URI handler (ymsgr:). This URI handler is installed at the system level for applications that use the underlying operating system when processing URIs (such as Microsoft Internet Explorer, Netscape Navigator 6, Microsoft Outlook, or the command shell). A URI can be sent by another Yahoo! Messenger user in a message, embedded in a web site, or sent in an HTML-renderable email message.

This vulnerability has been assigned as CAN-2002-0031 by the Common Vulnerabilities and Exposures (CVE) group:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0031>

VU#172315 - Yahoo! Messenger "addview" function allows for the automatic execution of malicious script contained in web pages

A vulnerability exists in the Yahoo! Messenger "addview" function that permits a remote attacker to execute arbitrary script and HTML in the Internet security zone of the local machine. The

"addview" function is only supposed to accept view information from Yahoo! servers. However, an attacker can send malicious script and HTML to the client using the Yahoo! URL redirection service. This script or HTML is interpreted by the Yahoo! Messenger client and is displayed in the client's web browser.

This vulnerability has been assigned as CAN-2002-0032 by the Common Vulnerabilities and Exposures (CVE) group:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0032>

These vulnerabilities were resolved in Yahoo! Messenger version 5,0,0,1065, released May 22, 2002; however, a bug in the distribution server may have inadvertently installed Yahoo! Messenger version 5,0,0,1036 on systems that downloaded Yahoo! Messenger after May 22, 2002. The bug in the distribution server has since been resolved.

In February 2002, the following vulnerabilities were reported to affect Yahoo! Messenger:

- <http://www.kb.cert.org/vuls/id/393195>
- <http://www.kb.cert.org/vuls/id/419419>
- <http://www.kb.cert.org/vuls/id/755755>
- <http://www.kb.cert.org/vuls/id/887319>
- <http://www.kb.cert.org/vuls/id/952875>

All of these vulnerabilities were resolved in Yahoo! Messenger version 5,0,0,1058, released February 25, 2002, or by server-side resolutions around the same time.

II. Impact

A remote attacker can execute arbitrary code with the privileges of the victim user, cause a denial of service, or modify data in the victim's buddy list.

III. Solution

Upgrade to the latest version of Yahoo! Messenger

On May 22, 2002, Yahoo! released a fixed version of Yahoo! Messenger (5,0,0,1065) in the United States and began issuing a patch (5,0,0,1066) via the AutoUpdater to address this issue. All users should upgrade to version 5,0,0,1065 or later. Users with versions prior to 5,0,0,1066 that have "Auto Update" enabled will receive a message informing them that an upgrade is available. All users should accept this upgrade.

All of the international clients have been updated and should be available for download from the regional web site. Users with International or branded versions prior to 5,0,0,1066 should upgrade to version 5,0,0,1065 or later of the native client from the regional web site.

Users who downloaded Yahoo! Messenger after May 22, 2002, should be aware that a bug in the distribution server may have inadvertently installed Yahoo! Messenger version 5,0,0,1036, which

is vulnerable to all issues in this advisory. The bug in the distribution server has since been resolved.

Users should upgrade and verify the version of Yahoo! Messenger by selecting the "About Yahoo! Messenger..." option from the Help menu.

Implement a firewall and filtering

Yahoo! Messenger runs a variety of services on several ports. Yahoo! Messenger typically listens for peer-to-peer requests on port 5101/TCP and client-to-server communications on 5050/TCP, but is not limited to these ports. Users can attempt to implement a firewall to block inbound and outbound access to port 5101/TCP, 5050/TCP, or any other port(s) that Yahoo! Messenger chooses to bind a service. However, the Yahoo! Messenger client will attempt to connect to the server through ports 20, 21, 25, 37, 80, and 119 if 5050 is blocked, therefore this may not be a viable nor practical solution for most sites.

Note also that since Yahoo! Messenger URI's can be embedded in a web site or email message, blocking requests to and from these ports is not a completely effective solution. Mail and Internet filters should also be applied to filter the "ymsgr:" URI handler from email messages and web sites.

Appendix A Vendor Information

This appendix contains information provided by vendors for this advisory. When vendors report new information to the CERT/CC, we update this section and note the changes in our revision history. If a particular vendor is not listed below, we have not received their comments.

Yahoo!, Inc.

Yahoo! encourages users to upgrade to the latest version whenever prompted by the AutoUpdater or regularly check for updated versions of the client at <http://messenger.yahoo.com>.

International users should also upgrade to version 5,0,0,1066 or later, which is available from their regional messenger download site. For example, <http://au.messenger.yahoo.com> for Australian users.

The CERT Coordination Center thanks Scott Woodward <scott@phoenixtechie.com>, Phuong Nguyen <dphuong@yahoo.com>, and Adam Lang <themeetup@hotmail.com> for their discovery and analysis of these vulnerabilities. We also thank Yahoo! for their assistance in analyzing and responding to these issues.

Feedback can be directed to the author: [Jason A. Rafail](mailto:Jason.A.Rafail).

Appendix B References

1. <http://www.kb.cert.org/vuls/id/137115>
2. <http://www.kb.cert.org/vuls/id/172315>

3. <http://www.kb.cert.org/vuls/id/393195>
4. <http://www.kb.cert.org/vuls/id/419419>
5. <http://www.kb.cert.org/vuls/id/755755>
6. <http://www.kb.cert.org/vuls/id/887319>
7. <http://www.kb.cert.org/vuls/id/952875>

Copyright 2002 Carnegie Mellon University

Revision History

June 05, 2002: Initial release

June 06, 2002: Updated information about ports and International versions

June 07, 2002: Updated information International versions

June 07, 2002: Updated information about ports and filtering

June 07, 2002: Updated Yahoo! vendor statement

17 CA-2002-17: Apache Web Server Chunk Handling Vulnerability

Original release date: June 17, 2002

Last revised: November 2, 2007

Source: CERT/CC

A complete revision history can be found at the end of this file.

Systems Affected

- Web servers based on Apache code versions 1.2.2 and above
- Web servers based on Apache code versions 1.3 through 1.3.24
- Web servers based on Apache code versions 2.0 through 2.0.36

Overview

There is a remotely exploitable vulnerability in the way that Apache web servers (or other web servers based on their source code) handle data encoded in chunks. This vulnerability is present by default in configurations of Apache web server versions 1.2.2 and above, 1.3 through 1.3.24, and versions 2.0 through 2.0.36. The impact of this vulnerability is dependent upon the software version and the hardware platform the server is running on.

I. Description

Apache is a popular web server that includes support for chunk-encoded data according to the HTTP 1.1 standard as described in [RFC2616](#). There is a vulnerability in the handling of certain chunk-encoded HTTP requests that may allow remote attackers to execute arbitrary code.

The Apache Software Foundation has published an advisory describing the details of this vulnerability. This advisory is available on their web site at http://httpd.apache.org/info/security_bulletin_20020617.txt.

Vulnerability Note [VU#944335](#) includes a list of vendors that have been contacted about this vulnerability.

II. Impact

For Apache versions 1.2.2 through 1.3.24 inclusive, this vulnerability may allow the execution of arbitrary code by remote attackers. Exploits are publicly available that claim to allow the execution of arbitrary code.

For Apache versions 2.0 through 2.0.36 inclusive, the condition causing the vulnerability is correctly detected and causes the child process to exit. Depending on a variety of factors, including

the threading model supported by the vulnerable system, this may lead to a denial-of-service attack against the Apache web server.

III. Solution

Upgrade to the latest version

The Apache Software Foundation has released two new versions of Apache that correct this vulnerability. System administrators can prevent the vulnerability from being exploited by upgrading to Apache httpd version 1.3.26 or 2.0.39.

Due to some unexpected problems with version 1.3.25, the CERT/CC has been informed by the Apache Software Foundation that the corrected version of the software is now 1.3.26. Both 1.3.26 and 2.0.39 are available on their web site at

<http://www.apache.org/dist/httpd/>

Apply a patch from your vendor

If your vendor has provided a patch to correct this vulnerability, you may want to apply that patch rather than upgrading your version of httpd. The CERT/CC is aware of a patch from ISS that corrects some of the impacts associated with this vulnerability. System administrators are encouraged to ensure that the patch they apply is based on the code by the Apache Software Foundation that also corrects additional impacts described in this advisory.

More information about vendor-specific patches can be found in the vendor section of this document. Because the publication of this advisory was unexpectedly accelerated, statements from all of the affected vendors were not available at publication time. As additional information from vendors becomes available, this document will be updated.

Appendix A Vendor Information

This appendix contains information provided by vendors for this advisory. As vendors report new information to the CERT/CC, we will update this section and note the changes in our revision history. If a particular vendor is not listed below, we have not received their comments.

Alcatel

In relation to this CERT advisory on security vulnerability in Apache, Alcatel has conducted an immediate assessment to determine any impact this may have on our portfolio. A first analysis has shown that various Alcatel products can be affected: namely the A5000 and A5020 SoftSwitches, the A5735 SMC, the A1300 NMC2, the management platforms for the A1000 UMTS/GPRS/MSR solutions, the 1353 SH and 1355 VP. Customers using these products should upgrade to Apache WebServer 1.3.26 (or higher) or may contact their Alcatel support rep-

representative for more details. The security of our customers' networks is of highest priority for Alcatel. Therefore we continue to test our product portfolio against potential security vulnerabilities in our products using the Apache Webserver and will provide updates if necessary.

Apache Software Foundation

New versions of the Apache software are available from: <http://httpd.apache.org/>.

Apple Computer, Inc.

This vulnerability is fixed with the release of the "Security Update - July 2002" software update.

Caldera

Caldera has published several advisories describing this vulnerability:

<ftp://ftp.caldera.com/pub/security/OpenLinux/CSSA-2002-029.0.txt>

<ftp://ftp.caldera.com/pub/security/OpenUNIX/CSSA-2002-SCO.31.txt>

<ftp://ftp.caldera.com/pub/security/UnixWare/CSSA-2002-SCO.31.txt>

<ftp://ftp.caldera.com/pub/security/OpenServer/CSSA-2002-SCO.32.txt>

Cisco Systems

Cisco Systems is evaluating the vulnerabilities identified by VU#944335. Should an issue be found, Cisco will release a Security Advisory. The most up-to-date information on all Cisco product security issues may be found at <http://www.cisco.com/go/psirt/>.

Compaq Computer Corporation

Compaq has released Security Bulletin [SSRT2253](#) (document number SRB0021W).

Conectiva Linux

The Apache webserver shipped with Conectiva Linux is vulnerable to this problem. New packages fixing this problem will be announced to our mailing list after an official fix becomes available.

Covalent

Covalent Technologies distributes products based on Apache 1.3 and Apache 2.0 that may be subject to this vulnerability. Covalent is currently creating patches to affected products. Covalent customers will be informed by email, and by postings at www.covalent.net/support when the patches are available.

Cray, Inc.

Cray, Inc. does not distribute Apache with any of its operating systems.

Engarde

Guardian Digital ships Apache in all version of EnGarde Secure Linux. EnGarde Secure Professional users may update using the GDSN. This issue was addressed in ESA-20020619-014 which may be found at http://www.linuxsecurity.com/advisories/other_advisory-2137.html.

F5 Networks

The following F5 Networks, Inc. products contain a vulnerable version of the Apache-based web server. Instructions for obtaining and installing a patch are available in the following locations.

[BIG-IP® platform](#)

[3-DNS® platform](#)

[EDGE-FX® platform](#)

[GLOBAL-SITE® platform](#)

Fujitsu

Fujitsu's UXP/V operating system does not support Apache and is therefore not affected by the vulnerability reported in VU#944335.

Hewlett-Packard Company

HP makes the Apache Server available for customers as a bundled software package called "HP Apache." New updates are available temporarily via ftp from a site located at hprc.external.hp.com.

When the new updates are available at www.software.hp.com, the Hewlett-Packard Company Security Bulletin HPSBUX0207-197 will be updated.

To retrieve the updates from the temporary ftp site, use a browser to connect to:

<ftp://apache:apache@192.170.19.51/>

or:

<ftp://apache:apache@hprc.external.hp.com/>

There are two subdirectories containing depots of swinstallable binaries with a ".t" extension, one for Apache 2.0.39 (11.00 and 11.11) and one for Apache 1.3.26 (11.00 and 11.11).

HP Virtualvault (HP-UX 11.04) patches are available from itrc.hp.com with ID's of PHSS_27361 and PHSS_27371.

For full details, see Hewlett-Packard Company Security Bulletin HPSBUX0207-197, available on itrc.hp.com. Search for "Apache chunk"

IBM Corporation

IBM makes the Apache Server available for AIX customers as a software package under the AIX-Linux Affinity initiative. This package is included on the AIX Toolbox for Linux Applications CD, and can be downloaded via the IBM Linux Affinity website. The currently available version of Apache Server is susceptible to the vulnerability described here. We will update our Apache Server offering shortly to version 1.3.23, including the patch for this vulnerability; this update will be made available for downloading by accessing this URL:

<http://www-1.ibm.com/servers/aix/products/aixos/linux/download.html> and following the instructions presented there.

Please note that Apache Server, and all Linux Affinity software, is offered on an "as-is" basis. IBM does not own the source code for this software, nor has it developed and fully tested this code. IBM does not support these software packages.

The IBM HTTP Server product, which is also bundled with the Websphere product, is based on the Apache server. As such, it is vulnerable to the current "Chunk Handling" issue and we are working on a patch for this problem with all due haste. This statement will be updated as more information becomes available.

Information for the Websphere patches is available from the web. Go to this URL:

<http://www.ibm.com/software/webservers/appserv/support.html>

Click on the "Websphere Flashes" link and look for the item for "IBM HTTP Server". This will contain information on the exposure and links to the patches.

The IBM HMC product is also affected by the Apache vulnerability described above. The HMC is the hardware monitor and control console used with IBM's Regatta systems. This is a separate hardware unit that uses a Linux-based operating system and Open Source software.

Customers are advised to obtain the latest security patches for the HMC. These patches will be available early next week from the following URL:

<http://techsupport.services.ibm.com/server/hmc?fetch=corrsrv.html>

Lotus

We have verified that the Lotus Domino web server is not vulnerable to this type of problem. Also, we do not ship Apache code with any Lotus products.

Microsoft Corporation

Microsoft does not ship the Apache web server.

Network Appliance

Data ONTAP(R) and NetCache(R) products are not affected.

ReplicatorX versions 4.0 through 4.0.21 are affected (This was originally released by Topio Inc, now a wholly owned subsidiary of NetApp, as Topio Data Protection Suite (TDPS) releases 1.0 through 3.0.65).

Contact the NetApp Technical Support Center +1-888-4NETAPP for remediation information and instructions.

Nortel Networks

Nortel Networks is reviewing its portfolio to determine if any products are affected by the vulnerability noted in CERT Advisory CA-2002-17. A definitive statement will be issued shortly.

Oracle

Oracle has issued Oracle Security Alert #36 in response to the chunked encoding Apache HTTP Server security vulnerability.

RedHat Inc.

Red Hat distributes Apache 1.3 versions in all Red Hat Linux distributions, and as part of Stronghold. However we do not distribute Apache for Windows. We are currently investigating the issue and will work on producing errata packages when an official fix for the problem is made available. When these updates are complete they will be available from the URL below. At the same time users of the Red Hat Network will be able to update their systems using the 'up2date' tool.

<http://rhn.redhat.com/errata/RHSA-2002-103.html>

Secure Computing Corporation

In response to the CERT Advisory CA-2002-17, Secure Computing has posted a software patch for users of the SafeWord PremierAccess version 3.1 authentication system. All existing and new customers are advised to download and apply PremierAccess Patch 1. Patch 1(v3.1.0.01) is available for immediate web download at

<http://www.securecomputing.com/index.cfm?skey=1109>.

SGI

SGI has released SGI Security Advisory [20020605-01-I](#).

Sun Microsystems Inc.

Sun bundles the Apache Web Server freeware product with Solaris 8 (Apache/1.3.12) and 9 (Apache/1.3.22). Both versions are affected by this vulnerability. Sun are presently producing

patches for this issue for Solaris 8 and 9. Once the patches are available, we will be publishing a Sun Alert available from:

<http://sunsolve.sun.com/>

Unisphere Networks

CUSTOMER SERVICE TECHNICAL BULLETIN

SUBJECT: CERT Advisory CA-2002-17: Apache Web Server Chunk Handling Vulnerability

BULLETIN NUMBER: SSC_PSN-001

BULLETIN TYPE: Product Support Notification

AFFECTED PRODUCTS: SSC

ISSUE DATE: 06/26/2002

REVISION: 1.0

PROBLEM DESCRIPTION:

The CERT Coordination Center released an advisory on June 17, 2002 entitled, "CERT Advisory CA-2002-17 Apache Web Server Chunk Handling Vulnerability". The URL for the full text of the advisory can be found at:

<http://www.cert.org/advisories/CA-2002-17.html>

AFFECTED PRODUCT(S):

SSC

SOLUTION:

The following releases of software have been found to suffer no negative effects from vulnerability outlined in CERT Advisory CA-2002-17:

2-0-2p2

2-0-3p2

All future releases of SSC will include the updated version of Apache web server that corrects this vulnerability.

Earlier releases of software may allow the execution of arbitrary code by remote attackers. Information needed to exploit this vulnerability is publicly known.

Affected releases include:

2-0-0 -- 2-0-2p1

2-0-3 -- 2-0-3p1

This Product Support Notification is publicly viewable on the Web at:

http://support.unispherenetworks.com/websupport/CERT/ssc_psn-001.pdf

If you have any questions concerning this notice, or to obtain the latest patch release, please contact Unisphere Networks Customer Service.

Inside the U.S. call: (800) 424-2344
Outside the U.S. call: (978) 589-9000
Via the Web @ <http://support.unispherenetworks.com>
Via email @ support@unispherenetworks.com

Trustix Secure Linux

Trustix Secure Linux has published an advisory on this topic:
<http://www.trustix.net/errata/misc/2002/TSL-2002-0056-apache.asc.txt>

Xerox

A response to this advisory is available from our web site: <http://www.xerox.com/security>.

The CERT/CC thanks Mark Litchfield for reporting this vulnerability to the Apache Software Foundation, and Mark Cox for reporting this vulnerability to the CERT/CC.

Author: Cory F. Cohen

Copyright 2002 Carnegie Mellon University

Revision History

June 17, 2002: Initial release
June 18, 2002: Added Fujitsu vendor statement.
June 18, 2002: Added information about Apache version 1.2.2 and above.
June 18, 2002: Added pointers to Apache versions including 1.3.26.
June 19, 2002: Added Covalent vendor statement.
June 19, 2002: Added Compaq vendor statement.
June 19, 2002: Added Engarde vendor statement.
June 19, 2002: Added SGI vendor statement.
June 19, 2002: Updated Solution section to clarify patch capabilities.
June 19, 2002: Added statement about exploit code for 32-bit platforms.
June 19, 2002: Try to be as clear as possible on the impact (all systems).
June 20, 2002: Added a link to the vulnerability note.
June 20, 2002: Added Hewlett-Packard vendor statement.
June 21, 2002: Added Oracle vendor statement.
June 24, 2002: Added F5 Networks vendor statement.
June 24, 2002: Updated IBM vendor statement to include Websphere information.
June 24, 2002: Added Sun Microsystems Inc. vendor statement.
June 27, 2002: Added Nortel vendor statement.

June 27, 2002: Updated Unisphere vendor statement.
June 28, 2002: Added Alcatel vendor statement.
June 28, 2002: Added Apple vendor statement.
July 08, 2002: Added Cisco vendor statement.
July 15, 2002: Updated Hewlett-Packard vendor statement.
July 15, 2002: Updated SGI vendor statement.
July 15, 2002: Added Caldera vendor statement.
July 15, 2002: Added Trustix vendor statement.
July 16, 2002: Updated Compaq vendor statement.
August 8, 2002: Added Xerox vendor statement.
August 8, 2002: Updated IBM vendor statement.
September 25, 2002: Added Secure Computing vendor statement.
March 27, 2003: Updated Xerox vendor statement.
November 2, 2007: Updated Network Appliance vendor statement.

18 CA-2002-18: OpenSSH Vulnerabilities in Challenge Response Handling

Original release date: June 26, 2002

Last revised: December 6, 2002

Source: CERT/CC

A complete revision history can be found at the end of this file.

Systems Affected

- OpenSSH versions 2.3.1p1 through 3.3

Overview

There are two related vulnerabilities in the challenge response handling code in OpenSSH versions 2.3.1p1 through 3.3. They may allow a remote intruder to execute arbitrary code as the user running sshd (often root). The first vulnerability affects OpenSSH versions 2.9.9 through 3.3 that have the challenge response option enabled and that use SKEY or BSD_AUTH authentication. The second vulnerability affects PAM modules using interactive keyboard authentication in OpenSSH versions 2.3.1p1 through 3.3, regardless of the challenge response option setting. Additionally, a number of other possible security problems have been corrected in OpenSSH version 3.4.

I. Description

Two related vulnerabilities have been found in the handling of challenge responses in OpenSSH.

The first vulnerability is an integer overflow in the handling of the number of responses received during challenge response authentication. If the challenge response configuration option is set to yes and the system is using SKEY or BSD_AUTH authentication then a remote intruder may be able to exploit the vulnerability to execute arbitrary code. This vulnerability is present in versions of OpenSSH 2.9.9 through 3.3. An exploit for this vulnerability is reported to exist. This vulnerability is partially described in a recent ISS security advisory available at

<http://bvlive01.iss.net/issEn/delivery/xforce/alertdetail.jsp?oid=20584>

The second vulnerability is a buffer overflow involving the number of responses received during challenge response authentication. Regardless of the setting of the challenge response configuration option, systems using PAM modules that use interactive keyboard authentication (PAMAuthenticationViaKbdInt), may be vulnerable to the remote execution of code. At this time, it is not known if this vulnerability is exploitable. Both vulnerabilities are corrected by the patches in a recent OpenSSH security advisory available from

<http://www.openssh.com/txt/preauth.adv>

Both vulnerabilities exploit features present only in version 2 of the SSH protocol.

Vulnerability Note VU#369347 lists the vendors we contacted about this vulnerability. The vulnerability note is available from <http://www.kb.cert.org/vuls/id/369347>.

II. Impact

A remote attacker can execute code with the privileges of the user running the sshd (often root). These vulnerabilities may also be used to cause a denial-of-service condition.

III. Solution

Upgrade to OpenSSH version 3.4

These vulnerabilities are eliminated by upgrading to OpenSSH version 3.4, which is available from the OpenSSH web site at <http://www.openssh.com> Appendix B.

OpenSSH version 3.4 will correct several other software defects with potential security implications not described in this advisory.

Apply a patch from your vendor

A patch for this problem is included in the OpenSSH advisory at <http://www.openssh.com/txt/preauth.adv>

This patch may be manually installed with minor changes to correct these vulnerabilities in all affected versions of OpenSSH. Please note that applying the patches described in the OpenSSH advisory does not correct the other software defects with potential security implications not described in this advisory.

If your vendor has provided a patch to correct these vulnerabilities, you may want to apply their patch rather than upgrading your version of sshd. System administrators may want to confirm whether their vendor's patch includes the other possible vulnerabilities corrected in OpenSSH 3.4. More information about vendor-specific patches can be found in the vendor section of this document. Because the publication of this advisory was unexpectedly accelerated, statements from all of the affected vendors were not available at publication time. We will update this document as vendors provide additional information.

Disable SSH protocol version 2

Since both vulnerabilities are present only in protocol version 2 features, disabling version 2 of the protocol will prevent both vulnerabilities from being exploited. Typically, this is accomplished by adding the following line to `/etc/ssh/sshd_config`:

```
Protocol 1
```


This option may set to "2,1" by default. System administrators should be aware that disabling protocol version 2 may prevent the sshd daemon from accepting connections in certain configurations. Applying one or both of the configuration changes described below may be a less disruptive workaround for this problem.

Disable challenge response authentication

For OpenSSH versions greater than 2.9, system administrators can disable the vulnerable portion of the code by setting the "ChallengeResponseAuthentication" configuration option to "no" in their sshd configuration file. Typically, this is accomplished by adding the following line to /etc/ssh/sshd_config:

```
ChallengeResponseAuthentication no
```

This option may be enabled (set to "yes") by default. This workaround should prevent the first vulnerability from being exploited if SKEY or BSD_AUTH authentication is used. It will **not** prevent the possible exploitation of the vulnerability via PAM interactive keyboard authentication.

Disable PAM authentication via interactive keyboard

For OpenSSH versions greater than 2.9, system administrators can disable the vulnerable portion of the code affecting the PAM authentication issue by setting the "PAMAuthenticationViaKbdInt" configuration option to "no" in their sshd configuration file. Typically, this is accomplished by adding the following line to /etc/ssh/sshd_config:

```
PAMAuthenticationViaKbdInt no
```

This option may be disabled (set to "no") by default. This workaround should prevent the second vulnerability from being exploited if PAM interactive keyboard authentication is used. It will **not** prevent the possible exploitation of the vulnerability via SKEY or BSD_AUTH authentication.

Disable both options in older versions of OpenSSH

For OpenSSH versions between 2.3.1p1 and 2.9, system administrators will instead need to set the following options in their ssh configuration file:

```
KbdInteractiveAuthentication no  
ChallengeResponseAuthentication no
```

Setting both of these options is believed to prevent the exploitation of the vulnerabilities regardless of which authentication mechanisms are used.

Use privilege separation to minimize impact

System administrators running OpenSSH versions 3.2 or 3.3 may be able to reduce the impact of this vulnerability by enabling the "UsePrivilegeSeparation" configuration option in their sshd configuration file. Typically, this is accomplished by adding the following line to /etc/ssh/sshd_config:

```
UsePrivilegeSeparation yes
```

This workaround does **not** prevent these vulnerabilities from being exploited, however due to the privilege separation mechanism, the intruder may be limited to a constrained chroot environment with restricted privileges. This workaround will not prevent these vulnerabilities from creating a denial-of-service condition. Not all operating system vendors have implemented the privilege separation code, and on some operating systems, it may limit the functionality of OpenSSH. System administrators are encouraged to carefully review the implications of using the workaround in their environment, and use a more comprehensive solution if one is available. The use of privilege separation to limit the impact of future vulnerabilities is encouraged.

Appendix A Vendor Information

This appendix contains information provided by vendors for this advisory. As vendors report new information to the CERT/CC, we will update this section and note the changes in our revision history. If a particular vendor is not listed below, we have not received their comments.

Alcatel

In relation to this CERT advisory on security vulnerabilities with OpenSSH implementation, Alcatel has conducted an immediate assessment to determine any impact this may have on our portfolio. An initial analysis has shown that none of our products is affected when used as delivered to customers. The security of our customers' networks is of highest priority for Alcatel. Therefore, updates will be provided if necessary. Customers may contact their Alcatel support representative for more details.

Apple Computer Inc.

These vulnerabilities are fixed with the release of the "Security Update - July 2002" software update.

Compaq Computer Corporation

Compaq has released Security Bulletin [SSRT2263](#) (document number SRB0022W).

Caldera

Caldera OpenLinux OpenSSH has neither the S/KEY nor BSD Auth features compiled in, so it is not vulnerable to the Challenge/Response vulnerability. We do have the ChallengeResponseAuthentication option on by default, however, so to be safe, we recommend that the option be disabled in the `sshd_config` file.

In addition, the `sshd_config` `PAMAuthenticationViaKbdInt` option is off by default, so OpenLinux is not vulnerable to the other alleged vulnerability in a default configuration, either. However, Caldera recommends that this option be disabled if it has been enabled by the system administrator.

Cisco

Cisco Systems is evaluating the vulnerabilities identified by VU#369347. Should an issue be found, Cisco will release a Security Advisory. The most up-to-date information on all Cisco product security issues may be found at

<http://www.cisco.com/go/psirt/>

Cray, Inc.

Cray, Inc. has found the OpenSSH released in Cray Open Software 3.0 to be vulnerable. Please see Field Notice 5105 and spr 722588 for fix information.

Debian

Debian 2.2 (the current stable release) is not affected by these problems. The current versions of our "testing" distribution, to become Debian 3.0, and our "unstable" distribution, are both affected by default.

We recommend that users be certain that both:

`ChallengeResponseAuthentication no`

and

`PAMAuthenticationViaKbdInt no`

are present and uncommented in `/etc/ssh/sshd_config` (and that the server is restarted). Also, we recommend the use of version 3.3p1, now available from security.debian.org (DSA-134). Stable users do not need to upgrade and may wish to wait until the packages have received better testing.

We intend to provide 3.4p1 packages in the near future.

Engarde

Guardian Digital ships OpenSSH in all versions of EnGarde Secure Linux. Version 3.3p1 was introduced by ESA-20020625-015 on June 25, 2002. This update introduces privilege separation. All users are strongly urged to upgrade to this version as soon as possible.

An upgrade to version 3.4p1 (which properly fixes the bugs) will be made available sometime in the next few days.

F5 Networks

The following versions of F5 Networks, Inc. products contain a vulnerable version of the OpenSSH server. Instructions for obtaining and installing a patch are available at the following locations:

BIG-IP® and 3-DNS® versions 4.2 through 4.3

GLOBAL-SITE® versions 2.2 through 3.0

EDGE-FX® versions 2.0 through 3.0

Software versions not listed above are not affected by this vulnerability.

FreeBSD

Please note that no released versions of FreeBSD-STABLE are vulnerable to either issue described in this advisory. See [FreeBSD-SA-02:31](#) for more information.

F-Secure

F-Secure SSH product versions are not affected by these vulnerabilities discussed in CERT Advisory CA-2002-18.

Fujitsu

Fujitsu's UXP/V operating system is not affected because it does not support any SSH package.

Hewlett-Packard Company

HP has issued a security bulletin (HPSBUX0206-195) for HP 9000 Servers running HP-UX release 11.00 and 11.11 only with the T1471AA SSH product installed.

It says in part:

As a short-term solution, disable PAMAuthenticationViaKbdInt in the sshd_config file; i.e.,

```
PAMAuthenticationViaKbdInt no
```

NOTE: ChallengeResponseAuthentication is not used in the HP product.

HP has issued Security Bulletin HPSBTL0207-050 for OpenSSH 3.1p1 running on HP Secure OS Software for Linux.

IBM Corporation

IBM's AIX operating system does not ship with OpenSSH; however, OpenSSH is available for installation on AIX via the Linux Affinity Toolkit. The version included on the CD containing the Toolkit is vulnerable to the latest discovered vulnerability discussed here as is the version of OpenSSH available for downloading from the IBM Linux Affinity website. Anyone running this version is advised to follow the recommendations above to limit their vulnerability.

We working with the changes for version 3.4 and will have a new package available for download as soon as possible. When available the new packages can be downloaded from:

<http://www6.software.ibm.com/dl/aixtbx/aixtbx-p>

This site contains Linux Affinity applications containing cryptographic algorithms, and new users of this site are asked to register first.

The IBM HMC product is also affected by the SSH vulnerability described above. The HMC is the hardware monitor and control console used with IBM's Regatta systems. This is a separate hardware unit that uses a Linux-based operating system and Open Source software.

Customers are advised to obtain the latest security patches for the HMC. These patches will be available early next week from the following URL: <http://techsupport.services.ibm.com/server/hmc?fetch=corrsrv.html>

Customers are advised to limit the use of SSH until these patches have been applied.

Juniper Networks

Although all domestically (i.e., United States) available releases of JUNOS Internet Software includes OpenSSH, the version of OpenSSH used is not susceptible to this vulnerability. There is therefore no need for customers to upgrade their JUNOS software.

OpenSSH is not included in any world-wide version of JUNOS, nor is it included in the Prisma G10 CMTS software release. Therefore, neither of these products are not susceptible to this vulnerability.

Lotus

Lotus products are not vulnerable to this problem.

Mandrake Software

MandrakeSoft released OpenSSH 3.3p1 in updates Monday night to mitigate this vulnerability. Updates to OpenSSH 3.4p1 will be available for download later this week.

Microsoft Corporation

Microsoft products are not affected by the issues detailed in this advisory.

NetBSD

The signed advisory is available at: <ftp://ftp.NetBSD.ORG/pub/NetBSD/security/advisories/NetBSD-SA2002-005.txt.asc>

Netscreen

NetScreen appliances and systems are not vulnerable to either issue mentioned in the referenced advisory. NetScreen products do not implement the challenge-response authentication methods described in the advisory.

Network Appliance

NetApp systems are not vulnerable to this problem.

Nortel Networks

Nortel Networks has concluded its portfolio review and has determined that the following two products are shipped with OpenSSH:

1. In STORM, release SN04, the challenge response authentication feature is not used and therefore Nortel Networks recommends that it be disabled, which will not impact the product. The recommendations in CERT Advisory CA-2002-18 to disable features should be followed.
2. The SFTP sshd server on the SuperNode Data Manager is not affected by the vulnerabilities noted in CERT Advisory CA-2002-18 because the challenge response and separation of privileges mechanisms are not enabled as shipped with ASG Passwerks v3.x.

The core OpenSSH distribution will be upgraded to v3.4 with the SN05 release.

For more information please contact Nortel at:

North America: 1-8004NORTEL or 1-800-466-7835

Europe, Middle East and Africa: 00800 8008 9009, or +44 (0) 870 907 9009

Contacts for other regions are available at

www.nortelnetworks.com/help/contact/global/

OpenBSD

See <http://www.openbsd.org/errata.html#sshd>

OpenPKG

The OpenPKG Project has released OpenPKG Security Advisory [OpenPKG-SA-2002.005](#).

OpenSSH

See <http://www.openssh.com/txt/preauth.adv>

Process Software

MultiNet, TCPware, and SSH for OpenVMS are not affected by the problems outlined in this advisory.

RedHat Inc.

Red Hat Linux versions 7, 7.1, 7.2 and 7.3 as well as Red Hat Linux Advanced Server version 2.1 ship with OpenSSH. The Red Hat Linux OpenSSH packages were not compiled with either `BSD_AUTH` or `SKEY` enabled, therefore in order to be vulnerable to this issue a user would need to have enabled the configuration option `"PAMAuthenticationViaKbdInt"` in their `sshd` configuration file (the default is disabled).

We are continuing to investigate this vulnerability and will release updated packages where appropriate.

SGI

At this time, SGI does not ship OpenSSH as a part of IRIX.

The OpenSSH privilege separation code mostly works with IRIX, but it uses a flag to `mmap` that isn't in IRIX (`MAP_ANON`) for compression so you can't have both on at the same time. IRIX doesn't ship with PAM so a lot of the PAM issues aren't issues for us.

Slackware

Slackware has upgraded to OpenSSH-3.4-p1. See the entry dated "Wed Jun 26 12:03:06 PDT 2002" in the [slackware-8.1](#), [slackware-8.0](#), and [slackware-7.1](#) ChangeLogs.

SSH Communications Security

SSH Communications Security Oyj.

SSH Secure Shell product versions are not affected by these vulnerabilities.

Sun Microsystems

The version of OpenSSH that is in Solaris 9 is not believed to be vulnerable if the default configuration is used. If `sshd_config(4)` has been updated so that BOTH of the following entries are present then it is vulnerable.

```
PAMAuthenticationViaKBDInt yes
KbdInteractiveAuthentication yes
```

Note that in the default `sshd_config(4)` `PAMAuthenticationViaKBDInt` is listed but `KbdInteractiveAuthentication` is not (the compiled in default for `KbdInteractiveAuthentication` is no).

Sun is in the process of producing a patch for Solaris 9. Older Solaris releases are not vulnerable since they do not include OpenSSH as part of the Solaris distribution - hosts that added OpenSSH as part of their own site configurations should check the official OpenSSH advisory for details.

The patch that Sun produces to fix this issue will not contain the new OpenSSH Privsep support as it is not yet stable enough on Solaris due to interactions with PAM and BSM auditing, this may

appear in a future release - Sun is working with the OpenSSH developers on the PAM problems and once a working OpenSSH with PAM and BSM is available we will re-evaluate our position on Privsep.

Sun will publish a Sun Security Bulletin and a Sun Alert for this issue. The Sun Alert will be available from: <http://sunsolve.sun.com>

The patch will be available from: <http://sunsolve.sun.com/securitypatch>

Sun Security Bulletins are available from: <http://sunsolve.sun.com/security>

SuSE Linux

[F]urther details about the bugs in question have turned up by now, indicating that SuSE Linux products are not affected to the mentioned problem unless the administrator of an openssh installation has actively added the configuration option (PAMAuthenticationViaKbdInt) to the daemon configuration file /etc/ssh/sshd_config to turn this option on. In other words: We are not vulnerable by default.

We have quickly published update packages with the workaround as described in your announcement, but due to incompatibilities and errors in the newer package, we think about downgrading back to our 2.9.9p2 version packages as well as one newer version on one of our newer products. The decision about the downgrade has not been made yet, but we are positive about that we will publish another set of update packages that effectively remove the weakness from the package. After all, the currently offered packages for download from our ftp server (<ftp://ftp.suse.com/pub/suse/i386/update/>) represent an emergency fix that should be considered incomplete considering the quality standards at SuSE.

Trustix Secure Linux

Trustix has released Trustix Secure Linux Security Advisory [#2002-0059](#).

Unisphere Networks

The SSH implementation used within the Unison OS found on the ERX and MRX product lines is based on a third-party product that has been confirmed to be invulnerable to the OpenSSH vulnerabilities outlined in CERT Advisory CA-2002-18.

Xerox

A response to this advisory is available from our web site: <http://www.xerox.com/security>.

The CERT/CC thanks Theo de Raadt and Markus Friedl of the OpenSSH project for their technical assistance in producing this advisory.

Author: [Cory F. Cohen](#)

Copyright 2002 Carnegie Mellon University

Revision History

June 26, 2002: Initial release
June 26, 2002: Added statement from SuSE which should have been in the original advisory
June 27, 2002: Added Fujitsu vendor statement.
June 27, 2002: Added F-Secure vendor statement.
June 27, 2002: Added SSH Communications Security vendor statement.
June 27, 2002: Added Netscreen vendor statement.
June 27, 2002: Updated Hewlett Packard vendor statement.
June 27, 2002: Added Nortel vendor statement.
July 02, 2002: Added Juniper Networks vendor statement.
July 02, 2002: Added Unisphere vendor statement.
July 02, 2002: Added Sun Microsystems vendor statement.
July 02, 2002: Added FreeBSD vendor statement.
July 02, 2002: Added Apple Computer Inc statement.
July 08, 2002: Added NetBSD vendor statement.
July 08, 2002: Added Cisco vendor statement.
July 16, 2002: Updated FreeBSD vendor statement.
July 16, 2002: Updated Hewlett Packard vendor statement.
July 16, 2002: Updated Nortel Networks vendor statement.
July 16, 2002: Updated Compaq vendor statement.
July 17, 2002: Added F5 Networks vendor statement.
July 17, 2002: Added Slackware vendor statement.
July 17, 2002: Added Trustix vendor statement.
July 17, 2002: Added OpenPKG vendor statement.
August 8, 2002: Added Alcatel vendor statement.
August 8, 2002: Updated IBM vendor statement.
December 6, 2002: Added Xerox vendor statement.

19 CA-2002-19: Buffer Overflows in Multiple DNS Resolver Libraries

Original release date: June 28, 2002

Last revised: November 19, 2008

Source: CERT/CC

A complete revision history can be found at the end of this file.

Systems Affected

Applications using vulnerable implementations of the Domain Name System (DNS) resolver libraries, which include, but are not limited to

- Internet Software Consortium (ISC) Berkeley Internet Name Domain (BIND) DNS resolver library (libbind)
- Berkeley Software Distribution (BSD) DNS resolver library (libc)
- GNU DNS resolver library (glibc)

Overview

Buffer overflow vulnerabilities exist in multiple implementations of DNS resolver libraries. Operating systems and applications that utilize vulnerable DNS resolver libraries may be affected. A remote attacker who is able to send malicious DNS responses could potentially exploit these vulnerabilities to execute arbitrary code or cause a denial of service on a vulnerable system.

I. Description

The DNS protocol provides name, address, and other information about Internet Protocol (IP) networks and devices. To access DNS information, a network application uses the resolver to perform DNS queries on its behalf. Resolver functionality is commonly implemented in libraries that are included with operating systems.

Multiple implementations of DNS resolver libraries contain remotely exploitable buffer overflow vulnerabilities in the code used to handle DNS responses. Both BSD (libc) and ISC BIND (libbind) resolver libraries share a common code base and are vulnerable to this problem; any DNS resolver implementation that derives code from either of these libraries may also be vulnerable. Network applications that use vulnerable resolver libraries are likely to be affected, therefore this problem is not limited to DNS or BIND servers.

Two sets of responses could trigger buffer overflows in vulnerable DNS resolver libraries: responses for host names or addresses, and responses for network names or addresses. The GNU glibc resolver addressed the vulnerability in handling responses for host resolution in version

2.1.3. However, versions of glibc prior to and including 2.2.5 are vulnerable to responses for network resolution, as explained below in the GNU glibc [vendor statement](#). BSD (libc) and ISC BIND (libbind) resolvers are vulnerable to both types of responses.

VU#803539 ([CAN-2002-0651](#)) lists vendors that have been contacted and provides further information about these vulnerabilities: <http://www.kb.cert.org/vuls/id/803539>

VU#542971 ([CAN-2002-0684](#)) describes the network name and address resolution vulnerability in the GNU libc library (glibc): <http://www.kb.cert.org/vuls/id/542971>

NetBSD Security Advisory 2002-006 also explains these vulnerabilities in detail: <ftp://ftp.NetBSD.ORG/pub/NetBSD/security/advisories/NetBSD-SA2002-006.txt.asc>

Note that these vulnerabilities are not related to the Sendmail DNS map issue discussed in [VU#814627](#).

II. Impact

An attacker who is able to send malicious DNS responses could remotely exploit these vulnerabilities to execute arbitrary code or cause a denial of service on vulnerable systems. Any code executed by the attacker would run with the privileges of the process that calls the vulnerable resolver function.

Note that an attacker could cause one of the victim's network services to make a DNS request to a DNS server under the attacker's control. This would permit the attacker to remotely exploit these vulnerabilities.

III. Solution

Upgrade to a corrected version of the DNS resolver libraries.

Note that DNS resolver libraries can be used by multiple applications on most systems. It may be necessary to upgrade or apply multiple patches and then recompile statically linked applications.

Applications that are *statically* linked must be recompiled using patched resolver libraries. Applications that are *dynamically* linked do not need to be recompiled; however, running services need to be restarted in order to use the patched resolver libraries.

System administrators should consider the following process when addressing this issue:

1. Patch or obtain updated resolver libraries.
2. Restart any dynamically linked services that use the resolver libraries.
3. Recompile any statically linked applications using the patched or updated resolver libraries.

Use of a local caching DNS server is not an effective workaround.

When this advisory was initially published, it was thought that a caching DNS server that reconstructs DNS responses would prevent malicious code from reaching systems with vulnerable resolver libraries.

This workaround is not sufficient. It does not prevent some DNS responses that contain malicious code from reaching clients, whether or not the responses are reconstructed by a local caching DNS server. DNS responses containing code that is capable of exploiting the vulnerabilities described in [VU#803539](#) and [VU#542971](#) can be cached and reconstructed before being transmitted to clients. Since the server may cache the responses, the malicious code could persist until the server's cache is purged or the entries expire.

The only complete solution to this problem is to upgrade to a corrected version of the DNS resolver libraries as noted above.

Appendix A Vendor Information

This appendix contains information provided by vendors for this advisory. When vendors report new information, this section is updated and the changes are noted in the revision history. If a vendor is not listed below, we have not received their comments.

Apple Computer, Inc.

Mac OS X and Mac OS X Server are not vulnerable to the issue described in this notice.

Caldera

Caldera OpenLinux is affected (glibc):

<ftp://ftp.caldera.com/pub/security/OpenLinux/CSSA-2002-034.1.txt>

Caldera UnixWare is affected:

<ftp://ftp.caldera.com/pub/security/UnixWare/CSSA-2002-SCO.37.txt>

Compaq

SOURCE: Compaq Computer Corporation, a wholly-owned subsidiary of Hewlett-Packard Company and Hewlett-Packard Company HP Services Software Security Response Team

x-ref:SSRT2270

[Compaq (Hewlett-Packard) has released a security bulletin ([SRB0039W/SSRT2275](#)) that addresses VU#803539 and other vulnerabilities.]

Conectiva

Conectiva Linux supported versions (6.0, 7.0 and 8) are not vulnerable to VU#803539 regarding glibc packages. Regarding VU#542971, these same versions of Conectiva Linux are vulnerable

but not in the default installation, since `/etc/nsswitch.conf` ships without the `dns` parameter in the "networks:" line.

Updated glibc packages which fix the second vulnerability, VU#542971, will be provided.

Please see Conectiva Linux Announcement [CLSA-2002:507 \(english\)](#).

Cray, Inc.

The DNS resolver code supplied by Cray, Inc. in Unicos and Unicos/mk is vulnerable. SPR 722619 has been opened to track this problem.

Debian

Debian is vulnerable to the second vulnerability [VU#542971]:

Debian 2.2 aka potato aka stable: glibc 2.1.3 does not contain the included patch

Debian woody aka testing: glibc 2.2.5 does not contain the included patch

Debian sid aka unstable: glibc 2.2.5 does not contain the included patch

We are working towards an updated library.

We are not vulnerable to the first vulnerability [VU#803539] as published in the CERT Advisory CA-2002-19, though.

djbdns

djbdns does not have these bugs. djbdns has never used any BIND-derived code. djbdns, including the djbdns client library, is covered by a \$500 security guarantee. The djbdns client library is free for use by other packages in place of BIND's libresolv. See <http://cr.yp.to/djbdns.html>.

Elsewhere in this advisory, CERT and the BIND company suggest that administrators do not need to rush to upgrade their libresolv-based clients if they are using BIND 9 caches. The idea is that (1) BIND 9 caches never put CNAME records into the answer section of a DNS packet except at the top and (2) the BIND company believes that these libresolv bugs cannot be triggered by answer sections with all CNAME records at the top.

dnscache, the caching component of djbdns, is like the BIND 9 cache in all relevant respects. Specifically, it never puts CNAME records into the answer section except at the top. (This is the normal behavior for DNS caches; BIND 4 and BIND 8 are abnormal.)

However, it is simply not true that clients are protected by caches. Attackers can send unusual packets directly to clients, using the same well-known techniques used to selectively forge DNS responses. I do not endorse the suggestion of relying on caches (whether BIND 9 or dnscache) as a "solution" to the libresolv bugs. All libresolv-based clients must be upgraded immediately.

There are exceptions. Sites that use a local dnscache on every machine, with local firewalls preventing forgery of 127.0.0.1 and with proper IP-address checks in client libraries, are immune to cache-to-client packet forgery, as are sites that use IPSEC. However, even at those sites, libresolv-based clients should be upgraded immediately; the ability of the cache to take control of client programs, rather than simply providing DNS data, is a violation of standard security policy.

FreeBSD

FreeBSD has released FreeBSD-SA-02:28.resolv:

<ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-02:28.resolv.asc>

GNU adns

adns is not derived from BIND libresolv. Furthermore, it does not support a gethostbyname-like interface (which is where the bug in BIND libresolv is). Therefore, it is not vulnerable.

For more information on GNU adns, see:

<http://www.gnu.org/software/adns/>

<http://www.chiark.greenend.org.uk/~ian/adns/>

GNU glibc

For resolving host names and addresses via DNS, Version 2.1.2 and earlier versions of the GNU C Library are vulnerable. Later versions are not vulnerable.

For the less commonly used action of resolving network names and addresses via DNS as per Internet RFC 1011, Version 2.2.5 and earlier versions are vulnerable.

To work around the problems, modify the file `/etc/nsswitch.conf` so that it contains "hosts:" and "networks:" lines that do not mention "dns". For example, you might use the following lines in your `/etc/nsswitch.conf` file:

```
# This "networks:" line omits "dns" to work around a bug in glibc
# 2.2.5 and earlier.
networks: files nisplus
```

```
# This "hosts:" line omits "dns" to work around a bug in glibc
2.1.2
# and earlier.
hosts: nisplus [NOTFOUND=return] files
```

Most GNU/Linux distributions with glibc 2.1.3 and later ship with a line like "networks: files" in `/etc/nsswitch.conf` and thus unless this line is changed they are not vulnerable.

To fix the problem instead of working around it, we suggest upgrading to Version 2.1.3 or later, and applying the following patch, taking care to relink any statically linked applications that use the affected functions. This patch can also be found at:

<http://sources.redhat.com/cgi-bin/cvsweb.cgi/libc/resolv/nss_dns/dns-network.c.diff?r1=1.10&r2=1.10.2.1&cvsroot=glibc>

```
=====
==
RCS file: /cvs/glibc/libc/resolv/nss_dns/dns-network.c,v
retrieving revision 1.10
retrieving revision 1.10.2.1
diff -u -r1.10 -r1.10.2.1
--- libc/resolv/nss_dns/dns-network.c 2001/07/06 04:55:39 1.10
+++ libc/resolv/nss_dns/dns-network.c 2002/07/02 09:38:29
1.10.2.1
@@ -328,7 +328,9 @@
 }
 cp += n;
 *alias_pointer++ = bp;
 - bp += strlen (bp) + 1;
 + n = strlen (bp) + 1;
 + bp += n;
 + linebuflen -= n;
 result->n_addrtype = class == C_IN ? AF_INET : AF_UNSPEC;
 ++have_answer;
 }
```

Guardian Digital

Please see EnGarde Secure Linux Security Advisory [ESA-20020724-018](#).

Hewlett-Packard Company

HEWLETT-PACKARD COMPANY SECURITY BULLETIN: HPSBUX0208-209

Originally issued: 12 Aug 2002

reference id: VU#803539, SSRT2316

HP Published Security Bulletin HPSBUX0208-209 with solutions for HP9000 Series 700/800 running HP-UX releases 11.00 and 11.11 (11i) with products using DNS resolver libraries, including, but not limited to, BINDv920.INETSVCS-BIND.

This bulletin is available from the HP IT Resource Center page at: <http://itrc.hp.com> "Maintenance and Support" then "Support Information Digests" and then "hp security bulletins archive" search for bulletin HPSBUX0208-209.

reference id: VU#542971

describes a specific aspect of this vulnerability as it affects the GNU libc library (glibc):

The glibc resolver used by HP Secure OS Software for Linux is vulnerable. Please see Hewlett-Packard Company Security Bulletin HPSBTL0207-053 for more information.

IBM Corporation

IBM is vulnerable to the above DNS stub resolver issues in both the 4.3 and 5.1 releases of AIX. A temporary patch is available through an efix package. Efixes are available from ftp.software.ibm.com/aix/efixes/security. See the README file in this directory for additional information on the efixes.

The following APARs will be available in the near future:

AIX 4.3.3: IY32719

AIX 5.1.0: IY32746

Internet Software Consortium

All versions of BIND 4 from 4.8.1 prior to BIND 4.9.9 are vulnerable.

All versions of BIND 8 prior to BIND 8.2.6 are vulnerable.

All versions of BIND 8.3.x prior to BIND 8.3.3 are vulnerable.

BIND versions BIND 9.2.0 and BIND 9.2.1 are vulnerable.

The status of BIND 4.8 is unknown, assume that it is vulnerable.

BIND versions BIND 9.0.x and BIND 9.1.x are not vulnerable.

'named' itself is not vulnerable.

Updated releases can be found at:

<ftp://ftp.isc.org/isc/bind/src/4.9.9/>

<ftp://ftp.isc.org/isc/bind/src/8.2.6/>

<ftp://ftp.isc.org/isc/bind/src/8.3.3/>

<ftp://ftp.isc.org/isc/bind/contrib/ntbind-8.3.3/>

BIND 9 contains a copy of the BIND 8.3.x resolver library (lib/bind). This will be updated with the next BIND 9 releases (9.2.2/9.3.0) in the meantime please use the original in BIND 8.3.3.

Vendors wishing additional patches should contact bind-bugs@isc.org.

Query about BIND 4 and BIND 8 should be addressed to bind-bugs@isc.org.

Query about BIND 9 should be addressed to bind9-bugs@isc.org.

Juniper Networks

All versions of Juniper Networks JUNOS software released prior to June 27, 2002, are potentially vulnerable to this bug. This includes JUNOS versions 4.x, 5.0R1 through 5.0R4, 5.1R1 through 5.1R4, 5.2R1 through 5.2R3, and 5.3R1 through 5.3R2. (All releases of JUNOS software with version 5.4 or higher are NOT vulnerable.) The bug has been corrected as of June 27, 2002, and all future software releases will contain the correction. All Juniper Networks customers are encouraged to contact JTAC, the Juniper Networks Technical Assistance Center by telephone at 1-888-314-JTAC, or by E-mail at support@juniper.net for details on the availability of corrected software.

MetaSolv

The resolver code embedded in the DNS Server (Based on ISC BIND 8.2.3) on both MetaSolv Policy Services 4.1 and 4.2 are vulnerable to CERT/CC Advisory CA-2002-19. This issue is being tracked by MetaSolv under Case #28230. The ISC Sanctioned Patches to 8.2.3 for this advisory have been compiled and applied, and will be available in Policy Services 4.2 Service Pack 1. Please contact MetaSolv Global Customer Care (supporthd@metasolv.com) for availability and assistance.

MandrakeSoft

Please see MandrakeSoft Security Advisory [MDKSA-2002:043](#) (BIND) and [MDKSA-2002:050](#) (glibc).

Microsoft

Microsoft products do not use the libraries in question. Microsoft products are not affected by this issue.

NetBSD

NetBSD has released NetBSD Security Advisory 2002-006:
<ftp://ftp.NetBSD.ORG/pub/NetBSD/security/advisories/NetBSD-SA2002-006.txt.asc>

Network Appliance

Some NetApp systems are vulnerable to this problem. Check NOW (<http://now.netapp.com>) for information on whether your system is vulnerable and the appropriate patch release that you should install.

Nortel Networks

The following Nortel Networks products are potentially affected by the vulnerability identified in CERT/CC Advisory CA-2002-19:

- NetID. A bulletin entitled "NetID BIND Bulletin", dated 7-12-02 has been issued and is available from the following Nortel Networks support contacts:

North America: 1-8004NORTEL or 1-800-466-7835

Europe, Middle East and Africa: 00800 8008 9009, or +44 (0) 870 907 9009

Contacts for other regions are available at www.nortelnetworks.com/help/contact/global/

- Optivity NMS, which uses Sun Solaris operating systems supplied by third parties. Nortel Networks recommends following the mitigating practices in Sun Microsystems Inc.'s Alert Notification. Implementing such practices will not adversely impact this Nortel Networks product.
- Also, the former Nortel Networks product Preside Policy Server divested to MetaSolv Software, Inc. in February 2002 uses BIND 8 and may be potentially affected.

OpenBSD

[T]he resolver libraries in question got copied far and wide. They used to have a hell of a lot of bugs in them.

Now might be a good time for people to compare each others' libraries to each other. I would urge them to compare against the OpenBSD ones, where we've spent a lot of time on, but of course we still missed this. But perhaps people can then share some around. Not everyone is going to move to the bind9 stuff, since it is very different.

OpenPKG

Please see OpenPKG Security Advisory [OpenPKG-SA-2002.006](#).

Openwall Project

No release or branch of Openwall GNU/*/Linux (Owl) is known to be affected, due to Olaf Kirch's fixes for this problem getting into the GNU C library more than two years ago.

The BIND 4.9.8-OW2 patch and BIND 4.9.9 release (and thus 4.9.9-OW1) include fixes for this vulnerability, originally developed by Jun-ichiro itojun Hagino of NetBSD. The updated patches are available at the usual location:

<http://www.openwall.com/bind/>

The BIND 4.9.x-OW patches provide certain security features which are not a part of ISC's now deprecated BIND 4 and are recommended for use by sites which chose to stick with BIND 4 for a little longer for whatever reason. They aren't a part of Owl.

[VU#542971]

No release or branch of Openwall GNU/*/Linux (Owl) is affected in default configuration as the "dns" NSS module isn't enabled for network lookups in our default `/etc/nsswitch.conf` file.

The defect in "dns" module has been corrected in Owl-current on 2002/07/04 and that fix is included in the snapshot from 2002/07/07.

Red Hat Inc.

Please see Red Hat Security Advisory [RHSA-2002:139](#) (glibc) and [RHSA-2002:133](#) (libbind).

Secure Computing Corporation

This is the official Secure Computing response to CERT Advisory CA-2002-19 Buffer Overflow in Multiple DNS Resolver Libraries. Note that we are currently supporting three different firewalls with different solutions to this vulnerability.

GAUNTLET (tm) FIREWALL & VPN (5.X and 6.0)

Gauntlet software users should contact their operating system vendor for a revised version of the library (on Solaris it is libresolv.so, on HP-UX it is libnss_dns.1) in question and apply it as soon as it is available.

GAUNTLET E-PPLIANCE FIREWALL & VPN (EPL 1.X and 2.0)

Gauntlet e-ppliance would be vulnerable to this theoretical attack. Secure Computing engineering is currently examining the issue in preparation for a patch for the e-ppliance 300 and 1000 (all versions).

SIDEWINDER(tm) FIREWALL & VPN (all releases including Sidewinder Appliance)

This buffer overflow vulnerability can not be exploited to gain access to, or gain any valuable information from a Sidewinder. An attack against one of the Sidewinder components using this vulnerability would yield no special privileges (such as root access, shell access, configuration information, etc.) due to Sidewinder's SecureOS(tm) Type Enforcement(tm) technology (TE).

None of Sidewinder's critical services (proxies, ACL engine, etc.) do direct DNS processing. Resolution is done by 'self contained' DNS resolver processes which are not granted Type Enforcement access to any of the services configuration data, nor could it access the data contained by the service sessions, nor even execute a shell. This process has no access to any system resources useful to an attacker. And of course, there is no useful concept of root privilege on Sidewinder.

Sendmail

Sendmail uses the BIND resolver API, and is commonly linked with the BIND resolver library (libbind). As a result, Sendmail could be leveraged to exploit this vulnerability.

Note that the DNS map problem that was addressed in Sendmail 8.12.5 is a different issue, which is described in VU#814627:

<http://www.kb.cert.org/vuls/id/814627>

The announcement for Sendmail 8.12.5 also references the DNS map problem:

<http://www.sendmail.org/8.12.5.html>

SGI

SGI IRIX is not vulnerable. Please see SGI Security Advisory [20020701-01-I](#) for more information.

Sun Microsystems

The Solaris DNS resolver library (libresolv.so) is affected by this issue in all currently supported versions of Solaris:

Solaris 2.5.1, 2.6, 7, 8, and 9

Sun has released patches as specified in Sun Alert ID [46042](#).

Sun Security Bulletins are available from:

<http://sunsolve.sun.com/security>

SuSE

Please see SUSE Security Announcement [SUSE-SA:2002:026](#) (previously located [here](#)). See also [SUSE Linux Enterprise Security](#).

Trustix

Please see Trustix Secure Linux Security Advisory [#2002-0061](#).

The CERT Coordination Center thanks Joost Pol of PINE-CERT, the FreeBSD Project, the NetBSD Project, and David Conrad of [Nominum](#) for information used in this document.

Feedback can be directed to the authors: [Art Manion](#) and [Jason A. Rafail](#).

Appendix B References

1. <http://www.pine.nl/advisories/pine-cert-20020601.asc>
2. <ftp://ftp.NetBSD.ORG/pub/NetBSD/security/advisories/NetBSD-SA2002-006.txt.asc>
3. <ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-02:28.resolv.asc>
4. http://www.gnu.org/manual/glibc-2.2.5/html_node/Name-Service-Switch.html#Name%20Service%20Switch

Copyright 2002 Carnegie Mellon University

Revision History

June 28, 2002: Initial release

June 29, 2002: Updated NetBSD references, added Sendmail statement, reformatted vendor statements, added CVE reference, added Juniper statement

June 30, 2002: Updated ISC statement

July 1, 2002: Added Apple, Sun, and Openwall statements

July 10, 2002: Added IBM statement and GNU glibc statements

July 18, 2002: Added reference to VU#542971, added description of network and host responses and glibc vulnerability, added Secure Computing statement, updated Thanks statement, added Name Service Switch reference

July 25, 2002: Added djvns, Nortel, HP, Trustix, SGI, Conectiva, SuSE, Red Hat, OpenPKG, and Guardian Digital statements, updated IBM statement

July 26, 2002: Added MetaSolv statement, updated HP statement

August 9, 2002: Updated Red Hat statement

August 14, 2002: Changed title to reflect plural "overflows", changed references to plural "vulnerabilities", re-ordered Description section, added firewall statement to caching DNS server workaround, updated HP, Conectiva, and Openwall statements, added SuSE URL, added Debian and MandrakeSoft statements, re-formatted fixed-width text

August 27, 2002: Deprecated caching DNS server workaround, updated Caldera statement

August 28, 2002: Updated ISC and Sun statements

September 9, 2002: Updated Compaq statement

November 19, 2008: Update SUSE statement

20 CA-2002-20: Multiple Vulnerabilities in CDE ToolTalk

Original release date: July 10, 2002

Last revised: November 7, 2002

Source: CERT/CC

A complete revision history can be found at the end of this file.

Systems Affected

- Systems running CDE ToolTalk

Overview

Two vulnerabilities have been discovered in the Common Desktop Environment (CDE) ToolTalk RPC database server. The first vulnerability could be used by a remote attacker to delete arbitrary files, cause a denial of service, or possibly execute arbitrary code or commands. The second vulnerability could allow a local attacker to overwrite arbitrary files with contents of the attacker's choice.

I. Description

The Common Desktop Environment (CDE) is an integrated graphical user interface that runs on UNIX and Linux operating systems. CDE ToolTalk is a message brokering system that provides an architecture for applications to communicate with each other across hosts and platforms. The ToolTalk RPC database server, `rpc.ttdbserverd`, manages communication between ToolTalk applications. For more information about CDE, see

<http://www.opengroup.org/cde/>

<http://www.opengroup.org/desktop/faq/>

This advisory addresses two new vulnerabilities in the CDE ToolTalk RPC database server. These vulnerabilities are summarized below and are described in further detail in their respective vulnerability notes. A list previously documented problems in CDE can be found in [Appendix B](#).

Both of these vulnerabilities were discovered and reported by CORE SECURITY TECHNOLOGIES and are described in [CORE-20020528](#).

VU#975403 - Common Desktop Environment (CDE) ToolTalk RPC database server (`rpc.ttdbserverd`) does not adequately validate file descriptor argument to `_TT_ISCLOSE()`

The ToolTalk RPC database server does not validate the range of an argument passed to the procedure `_TT_ISCLOSE()`. As a result, certain locations in memory can be overwritten with zeros. For more information, please see [VU#975403](#):

<http://www.kb.cert.org/vuls/id/975403>

This vulnerability has been assigned [CAN-2002-0677](#) by the Common Vulnerabilities and Exposures (CVE) group.

VU#299816 - Common Desktop Environment (CDE) ToolTalk RPC database server (`rpc.ttdbserverd`) does not adequately validate file operations

The ToolTalk RPC database server does not ensure that the target of a file write operation is a valid file and not a symbolic link. For more information, please see [VU#299816](#):

<http://www.kb.cert.org/vuls/id/299816>

This vulnerability has been assigned [CAN-2002-0678](#) by the Common Vulnerabilities and Exposures (CVE) group.

II. Impact

VU#975403 - Common Desktop Environment (CDE) ToolTalk RPC database server (`rpc.ttdbserverd`) does not adequately validate file descriptor argument to `_TT_ISCLOSE()`

By issuing a specially crafted call to the procedure `_TT_ISCLOSE()`, a remote attacker could overwrite certain locations in memory with zeros. Using a combination of techniques that include valid ToolTalk RPC requests, an attacker could leverage this vulnerability to delete any file that is accessible by the ToolTalk RPC database server. Since the server typically runs with root privileges, any file on a vulnerable system could be deleted. Overwriting memory or deleting files could cause a denial of service. It may also be possible to execute arbitrary code and commands.

VU#299816 - Common Desktop Environment (CDE) ToolTalk RPC database server (`rpc.ttdbserverd`) does not adequately validate file operations

By referencing a specially crafted symbolic link in certain ToolTalk RPC requests, a local attacker could overwrite any file that is accessible by the the ToolTalk RPC database server with contents of the attacker's choice. Since the server typically runs with root privileges, any file on a vulnerable system could be overwritten. Overwriting root-owned files could lead to lead to privilege escalation or cause a denial of service.

III. Solution

Apply a patch from your vendor

[Appendix A](#) contains information provided by vendors for this advisory. As vendors report new information to the CERT/CC, we will update this section and note the changes in our revision history. If a particular vendor is not listed below, we have not received their comments. Please contact your vendor directly.

Disable vulnerable service

Until patches are available and can be applied, you may wish to disable the ToolTalk RPC database service. As a best practice, the CERT/CC recommends disabling all services that are not explicitly required. On a typical CDE system, it should be possible to disable `rpc.ttdbserverd` by commenting out the relevant entries in `/etc/inetd.conf` and if necessary, `/etc/rpc`, and then by restarting the `inetd` process.

The program number for the ToolTalk RPC database server is 100083. If references to 100083 or `rpc.ttdbserverd` appear in `/etc/inetd.conf` or `/etc/rpc` or in output from the `rpcinfo(1M)` and `ps(1)` commands, then the ToolTalk RPC database server may be running.

The following example was taken from a system running SunOS 5.8 (Solaris 8):

```
/etc/inetd.conf
...
#
# Sun ToolTalk Database Server
#
100083/1 tli rpc/tcp wait root /usr/dt/bin/rpc.ttdbserverd rpc.ttdb-
serverd
...
# rpcinfo -p
  program vers proto port service
  ...
  100083 1 tcp 32773
  ...
# ps -ef
  UID PID PPID C STIME TTY TIME CMD
  ...
  root 355 164 0 19:31:27 ? 0:00 rpc.ttdbserverd
  ...
```

Before deciding to disable the ToolTalk RPC database server or the RPC portmapper service, carefully consider your network configuration and service requirements.

Block access to vulnerable service

Until patches are available and can be applied, you may wish to block access to the ToolTalk RPC database server and possibly the RPC portmapper service from untrusted networks such as the Internet. Use a firewall or other packet-filtering technology to block the appropriate network ports. The ToolTalk RPC database server may be configured to use port 692/tcp or another port as indicated in output from the `rpcinfo(1M)` command. In the example above, the ToolTalk RPC database server is configured to use port 32773/tcp. The RPC portmapper service typically runs on ports 111/tcp and 111/udp. Keep in mind that blocking ports at a network perimeter does not protect the vulnerable service from attacks that originate from the internal network.

Before deciding to block or restrict access to the ToolTalk RPC database server or the RPC portmapper service, carefully consider your network configuration and service requirements.

Appendix A Vendor Information

This appendix contains information provided by vendors for this advisory. As vendors report new information to the CERT/CC, we will update this section and note the changes in our revision history. If a particular vendor is not listed below, we have not received their comments.

Caldera, Inc.

Caldera Open UNIX and Caldera UnixWare provide the CDE `ttdbserverd` daemon, and are vulnerable to these issues. Please see Caldera Security Advisory [CSSA-2002-SCO.28](#) for more information.

SCO OpenServer and Caldera OpenLinux do not provide CDE, and are therefore not vulnerable.

Compaq Computer Corporation

SOURCE: Compaq Computer Corporation, a wholly-owned subsidiary of Hewlett-Packard Company and Hewlett-Packard Company HP Services Software Security Response Team

CROSS REFERENCE: SSRT2251

[Compaq (Hewlett-Packard) has released a security bulletin ([SRB0039W/SSRT2251](#)) that addresses VU#975403, VU#299816, and other vulnerabilities.]

A recommended workaround however is to disable `rpc.ttdbserver` until solutions are available. This should only create a potential problem for public software packages applications that use the RPC-based ToolTalk database server. This step should be evaluated against the risks identified, your security measures environment, and potential impact of other products that may use the ToolTalk database server.

To disable `rpc.ttdbserverd`:

- Comment out the following line in `/etc/inetd.conf`:

```
rpc.ttdbserverd stream tcp swait root
/usr/dt/bin/rpc.ttdbserverd rpc.ttdbserverd
```
- Force `inetd` to re-read the configuration file by executing the `inetd -h` command.

Note: The internet daemon should kill the currently running `rpc.ttdbserver`. If not, manually kill any existing `rpc.ttdbserverd` process.

Cray, Inc.

Cray, Inc. does include ToolTalk within the CrayTools product. However, `rpc.ttdbserverd` is not turned on or used by any Cray provided application. Since a site may have turned this on for their own use, they can always remove the binary `/opt/ctl/bin/rpc.ttdbserverd` if they are concerned.

Fujitsu

Fujitsu's UXP/V operating system is not affected by the vulnerability reported in VU#975403 [or VU#299816] because UXP/V does not support any CDE functionalities.

Hewlett-Packard Company

HP9000 Series 700/800 running HP-UX releases 10.10, 10.20, 11.00, and 11.11 are vulnerable.

Until patches are available, install the appropriate file to replace `rpc.ttdbserver`.

Download `rpc.ttdbserver.tar.gz` from the ftp site. This file is temporary and will be deleted when patches are available from the standard HP web sites, including itrc.hp.com.

System: `hprc.external.hp.com (192.170.19.51)`

Login: `ttdb1`

Password: `ttdb1`

FTP Access: <ftp://ttdb1:ttdb1@hprc.external.hp.com/>

<ftp://ttdb1:ttdb1@192.170.19.51/>

File: `rpc.ttdbserver.tar.gz`

MD5: `da1be3aaf70d0e2393bd9a03feaf4b1d`

Hewlett-Packard has also released HP-UX Security Bulletin HPSBUX0207-199.

IBM Corporation

The CDE desktop product shipped with AIX is vulnerable to both the issues detailed above in the advisory. This affects AIX releases 4.3.3 and 5.1.0. An efix package will be available shortly from the IBM software ftp site. The efix packages can be downloaded from [ftp.software.ibm.com/aix/efixes/security](ftp://ftp.software.ibm.com/aix/efixes/security). This directory contains a README file that gives further details on the efix packages.

The following APARs will be available in the near future:

AIX 4.3.3: IY32368

AIX 5.1.0: IY32370

SGI

Please see SGI Security Advisories [20021101-01-P](#) (CDE ToolTalk) and [20021102-01-P](#) (IRIX ToolTalk).

Sun Microsystems, Inc.

The Solaris RPC-based ToolTalk database server, `rpc.ttdbserver`, is vulnerable to the two vulnerabilities [VU#975403 VU#299816] described in this advisory in all currently supported versions of Solaris:

Solaris 2.5.1, 2.6, 7, 8, and 9

Patches are being generated for all of the above releases. Sun will publish a Sun Security Bulletin and a Sun Alert for this issue. The Sun Alert will be available from:

<http://sunsolve.sun.com>

The patches will be available from:

<http://sunsolve.sun.com/securitypatch>

Sun Security Bulletins are available from:

<http://sunsolve.sun.com/security>

Xi Graphics

Xi Graphics deXtop CDE v2.1 is vulnerable to this attack. When announced, the update and accompanying text file will be:

<ftp://ftp.xig.com/pub/updates/dextop/2.1/DEX2100.016.tar.gz>

<ftp://ftp.xig.com/pub/updates/dextop/2.1/DEX2100.016.txt>

Most sites do not need to use the ToolTalk server daemon. Xi Graphics Security recommends that non-essential services are never enabled. To disable the ToolTalk server on your system, edit `/etc/inetd.conf` and comment out, or remove, the 'rpc.ttdbserver' line. Then, either restart `inetd`, or reboot your machine.

Appendix B References

- <http://www.opengroup.org/cde/>
- <http://www.opengroup.org/desktop/faq/>
- <http://www.cert.org/advisories/CA-2002-01.html>
- <http://www.cert.org/advisories/CA-2001-31.html>
- <http://www.kb.cert.org/vuls/id/172583>
- <http://www.cert.org/advisories/CA-2001-27.html>
- <http://www.kb.cert.org/vuls/id/595507>
- <http://www.kb.cert.org/vuls/id/860296>
- <http://www.cert.org/advisories/CA-1999-11.html>
- <http://www.cert.org/advisories/CA-1998-11.html>
- <http://www.cert.org/advisories/CA-1998-02.html>
- <http://www.corest.com/common/showdoc.php?id=251&idxseccion=10>

The CERT Coordination Center thanks the reporters, Iván Arce and Ricardo Quesada of CORE SECURITY TECHNOLOGIES, for their assistance and cooperation in producing this document.

Author: Art Manion

Copyright 2002 Carnegie Mellon University

Revision History

July 10, 2002: Initial release

July 11, 2002: Fixed formatting, added link to CORE-20020528, updated Caldera statement, corrected Fujitsu statement to read "is not affected"

July 19, 2002: Updated HP statement

September 9, 2002: Updated Compaq statement

November 5, 2002: Updated SGI statement (CDE ToolTalk)

November 7, 2002: Updated SGI statement (IRIX ToolTalk)

21 CA-2002-21: Vulnerability in PHP

Original release date: July 22, 2002

Last revised: Thu Jul 25 09:23:27 EDT 2002

Source: CERT/CC

A complete revision history can be found at the end of this file.

Systems Affected

- Systems running PHP versions 4.2.0 or 4.2.1

Overview

A vulnerability has been discovered in PHP. This vulnerability could be used by a remote attacker to execute arbitrary code or crash PHP and/or the web server.

I. Description

PHP is a popular scripting language in widespread use. For more information about PHP, see <http://www.php.net/manual/en/faq.general.php>.

The vulnerability occurs in the portion of PHP code responsible for handling file uploads, specifically multipart/form-data. By sending a specially crafted POST request to the web server, an attacker can corrupt the internal data structures used by PHP. Specifically, an intruder can cause an improperly initialized memory structure to be freed. In most cases, an intruder can use this flaw to crash PHP or the web server. Under some circumstances, an intruder may be able to take advantage of this flaw to execute arbitrary code with the privileges of the web server.

You may be aware that freeing memory at inappropriate times in some implementations of malloc and free does not usually result in the execution of arbitrary code. However, because PHP utilizes its own memory management system, the implementation of malloc and free is irrelevant to this problem.

Stefan Esser of e-matters GmbH has indicated that intruders *cannot* execute code on x86 systems. However, we encourage system administrators to apply patches on x86 systems as well to guard against denial-of-service attacks and as-yet-unknown attack techniques that may permit the execution of code on x86 architectures.

This vulnerability was discovered by e-matters GmbH and is described in detail in their [advisory](#). The PHP Group has also issued an [advisory](#). A list of vendors contacted by the CERT/CC and their status regarding this vulnerability is available in [VU#929115](#).

Although this vulnerability only affects PHP 4.2.0 and 4.2.1, e-matters GmbH has previously identified vulnerabilities in older versions of PHP. If you are running older versions of PHP, we encourage you to review <http://security.e-matters.de/advisories/012002.html>

II. Impact

A remote attacker can execute arbitrary code on a vulnerable system. An attacker may not be able to execute code on x86 architectures due to the way the stack is structured. However, an attacker can leverage this vulnerability to crash PHP and/or the web server running on an x86 architecture.

III. Solution

Apply a patch from your vendor

Appendix A contains information provided by vendors for this advisory. As vendors report new information to the CERT/CC, we will update this section and note the changes in our revision history. If a particular vendor is not listed below, we have not received their comments. Please contact your vendor directly.

Upgrade to the latest version of PHP

If a patch is not available from your vendor, upgrade to version 4.2.2.

Deny POST requests

Until patches or an update can be applied, you may wish to deny POST requests. The following workaround is taken from the PHP Security Advisory:

If the PHP applications on an affected web server do not rely on HTTP POST input from user agents, it is often possible to deny POST requests on the web server.

In the Apache web server, for example, this is possible with the following code included in the main configuration file or a top-level .htaccess file:

```
<Limit POST>
  Order deny,allow
  Deny from all
</Limit>
```

Note that an existing configuration and/or .htaccess file may have parameters contradicting the example given above.

Disable vulnerable service

Until you can upgrade or apply patches, you may wish to disable PHP. As a best practice, the CERT/CC recommends disabling all services that are not explicitly required. Before deciding to disable PHP, carefully consider your service requirements.

Appendix A Vendor Information

This appendix contains information provided by vendors for this advisory. As vendors report new information to the CERT/CC, we will update this section and note the changes in our revision history. If a particular vendor is not listed below, we have not received their comments.

Apple Computer Inc.

Mac OS X and Mac OS X Server are shipping with PHP version 4.1.2 which does not contain the vulnerability described in this alert.

Caldera

Caldera OpenLinux does not provide either vulnerable version (4.2.0, 4.2.1) of PHP in their products. Therefore, Caldera products are not vulnerable to this issue.

Compaq Computer Corporation

We have verified that this problem is not present on our distributions for HP Tru64 UNIX or HP OpenVMS products.

Conectiva

PHP 4.2.x is not shipped with Conectiva Linux.

Cray Inc.

Cray, Inc. does not supply PHP on any of its systems.

Debian

Debian GNU/Linux stable aka 3.0 is not vulnerable.
Debian GNU/Linux testing is not vulnerable.
Debian GNU/Linux unstable is vulnerable.

The problem affects PHP versions 4.2.0 and 4.2.1. Woody ships an older version of PHP (4.1.2), that doesn't contain the vulnerable function.

F5 Networks, Inc.

F5 Networks products do not include PHP 4.2.0 or 4.2.1, and are therefore not affected by this vulnerability.

FreeBSD

FreeBSD does not include any version of PHP by default, and so is not vulnerable; however, the FreeBSD Ports Collection does contain the PHP4 package. Updates to the PHP4 package are in progress and a corrected package will be available in the near future.

Guardian Digital

Guardian Digital has not shipped PHP 4.2.x in any versions of EnGarde, therefore we are not believed to be vulnerable at this time.

Hewlett-Packard Company

SOURCE: Hewlett-Packard Company Security Response Team

At the time of writing this document, Hewlett Packard is currently investigating the potential impact to HP's released Operating System software products.

As further information becomes available HP will provide notice of the availability of any necessary patches through standard security bulletin announcements and be available from your normal HP Services support channel.

IBM

IBM is not vulnerable to the above vulnerabilities in PHP. We do supply the PHP packages for AIX through the AIX Toolbox for Linux Applications. However, these packages are at 4.0.6 and also incorporate the security patch from 2/27/2002.

Mandrakesoft

Mandrake Linux does not ship with PHP version 4.2.x and as such is not vulnerable. The Mandrake Linux cooker does currently contain PHP 4.2.1 and will be updated shortly, but cooker should not be used in a production environment and no advisory will be issued.

Microsoft Corporation

Microsoft products are not affected by the issues detailed in this advisory.

Network Appliance

No Netapp products are vulnerable to this.

Red Hat Inc.

None of our commercial releases ship with vulnerable versions of PHP (4.2.0, 4.2.1).

SGI

SGI acknowledges the PHP vulnerability reported by CERT and is currently investigating. PHP does not currently ship as part of IRIX so SGI can confirm that base IRIX is not vulnerable. No further information is available at this time.

For the protection of all our customers, SGI does not disclose, discuss or confirm vulnerabilities until a full investigation has occurred and any necessary patch(es) or release streams are available for all vulnerable and supported IRIX operating systems. Until SGI has more definitive information to provide, customers are encouraged to assume all security vulnerabilities as exploitable and take appropriate steps according to local site security policies and requirements. As further information becomes available, additional advisories will be issued via the normal SGI security information distribution methods including the wiretap mailing list on <http://www.sgi.com/support/security/>.

SuSE Inc.

SuSE Linux is not vulnerable to this problem, as we do not ship PHP 4.2.x.

Trustix

The TSL team states that none of the versions of the Trustix Secure Linux distribution is vulnerable to the php 4.2.{0,1} vulnerability (CA-2002-21) as none of the TSL versions is shipped with php 4.2.x.

The CERT/CC acknowledges e-matters GmbH for discovering and reporting this vulnerability.

Author: [Ian A. Finlay](#)

Copyright 2002 Carnegie Mellon University

Revision History

July 22, 2002: Initial release
July 23, 2002: Added vendor statement for F5 Networks, Inc.
July 23, 2002: Added vendor statement for Conectiva
July 24, 2002: Added vendor statement for Trustix
July 24, 2002: Added vendor statement for SGI
July 25, 2002: Updated vendor statement for Compaq Computer Corporation

22 CA-2002-22: Multiple Vulnerabilities in Microsoft SQL Server

Original release date: July 29, 2002

Last revised: February 5, 2003

Source: CERT/CC

A complete revision history can be found at the end of this file.

Systems Affected

- Microsoft SQL Server 7.0
- Microsoft SQL Server 2000
- Microsoft Desktop Engine (MSDE) 2000
- Any application that includes MSDE

Overview

The Microsoft SQL Server contains several serious vulnerabilities that allow remote attackers to obtain sensitive information, alter database content, compromise SQL servers, and, in some configurations, compromise server hosts. These vulnerabilities are public and have been addressed by Microsoft Security Bulletins, but we believe their collective severity warrants additional attention.

I. Description

Since December 2001, Microsoft has published eight Microsoft Security Bulletins regarding more than a dozen vulnerabilities in the Microsoft SQL Server. This document provides information on the five most serious of these vulnerabilities; references to the remainder are provided in Appendix B.

In isolation, many of these vulnerabilities have significant preconditions that are difficult for an attacker to overcome. However, when exploited in combination, they allow attackers to gain additional flexibility and increase their chances for success. In particular, the privilege escalation vulnerability described in VU#796313 allows an attacker to weaken the security policy of the SQL server by granting it the same privileges as the operating system. With full administrative privileges, a compromised Microsoft SQL Server can be used to take control of the server host.

The CERT/CC encourages system administrators to take this opportunity to review the security of their Microsoft SQL servers and to apply the appropriate patches from the Microsoft bulletins listed in Appendix B.

VU#796313 - Microsoft SQL Server service account registry key has weak permissions that permit escalation of privileges (CAN-2002-0642)

The Microsoft SQL Server typically runs under a dedicated "service account" that is defined by system administrators at installation time. This definition is stored in the Windows registry with permissions that allow the SQL Server to change the value of the registry key. As a result, attackers with access to the "xp_regwrite" extended stored procedure can alter this registry key and cause the SQL Server to use the LocalSystem account as its service account.

Upon rebooting the server host or restarting the SQL service, the SQL Server will run with the full administrative privileges of the LocalSystem account. This ability allows a remote attacker to submit SQL queries that can execute any command on the system with the privileges of the operating system.

VU#225555 - Microsoft SQL Server contains buffer overflow in pwencrypt() function (CAN-2002-0624)

The Microsoft SQL Server provides multiple methods for users to authenticate to SQL databases. When SQL Server Authentication is used, the username and password of each database user is stored in a database on the SQL server. When users supply a password to the server using this method, a function named pwencrypt() is responsible for encrypting the user-supplied password so that it can be compared to the encrypted password stored on the SQL server.

There is a buffer overflow in pwencrypt() that allows remote attackers to execute arbitrary code on the SQL server by supplying a crafted password value. Successful exploitation of this vulnerability requires knowledge of a valid username and will cause the supplied code to execute with the privileges of the SQL service account.

VU#627275 - Microsoft SQL Server extended stored procedures contain buffer overflows (CAN-2002-0154)

Microsoft SQL Server provides a scripting construct known as an "extended stored procedure" that can execute a collection of server commands together. Several of the extended stored procedures included with the Microsoft SQL Server contain buffer overflow vulnerabilities. These procedures provide increased functionality for database applications, allowing them to access operating system or network resources.

Parameters are passed to extended stored procedures via an API that specifies the actual and maximum length of various parameter data types. Some of the extended stored procedures fail to adequately validate the length of input parameters, resulting in stack buffer overflow conditions.

Since some of the vulnerable procedures are configured by default to allow public access, it is possible for an unauthenticated attacker to exploit one or more of these buffer overflows. SQL Server databases are commonly used in web applications, so the vulnerable procedures may be accessible via the Internet. Microsoft Security Bulletin [MS02-020](#) states

An attacker could exploit this vulnerability in one of two ways. Firstly, the attacker could attempt to load and execute a database query that calls one of the affected functions. Secondly, if a website or other database front-end were configured to access and process arbitrary queries, it could be possible for the attacker to provide inputs that would cause the query to call one of the functions in question with the appropriate malformed parameters.

VU#399260 - Microsoft SQL Server 2000 contains heap buffer overflow in SQL Server Resolution Service (CAN-2002-0649)

The SQL Server Resolution Service (SSRS) was introduced in Microsoft SQL Server 2000 to provide referral services for multiple server instances running on the same machine. The service listens for requests on UDP port 1434 and returns the IP address and port number of the SQL server instance that provides access to the requested database.

The SSRS contains a heap buffer overflow that allows unauthenticated remote attackers to execute arbitrary code by sending a crafted request to port 1434/udp. The code within such a request will be executed by the server host with the privileges of the SQL Server service account.

VU#484891 - Microsoft SQL Server 2000 contains stack buffer overflow in SQL Server Resolution Service (CAN-2002-0649)

The SSRS also contains a stack buffer overflow that allows unauthenticated remote attackers to execute arbitrary code by sending a crafted request to port 1434/udp. The code within such a request will be executed by the server host with the privileges of the SQL Server service account.

II. Impact

VU#796313 - Microsoft SQL Server service account registry key has weak permissions that permit escalation of privileges

As a precondition, this vulnerability requires the ability to modify the SQL service account registry key (for example, via the "xp_regwrite" extended stored procedure). Attackers must convince an administrator to grant this access, or they must obtain it by exploiting one of the vulnerabilities listed in this advisory.

This vulnerability allows attackers to weaken the security policy of the SQL Server by elevating its privileges and causing it to run in the LocalSystem security context. As a side effect, it increases the severity of the other vulnerabilities listed in this advisory and may enable attackers to compromise the server host as well.

VU#225555 - Microsoft SQL Server contains buffer overflow in pwdencrypt() function

This vulnerability allows remote attackers with knowledge of a valid username to execute arbitrary code with the privileges of the SQL service account.

VU#627275 - Microsoft SQL Server extended stored procedures contain buffer overflows

This vulnerability allows unauthenticated remote attackers to execute arbitrary code with the privileges of the SQL service account.

VU#399260 - Microsoft SQL Server 2000 contains heap buffer overflow in SQL Server Resolution Service

This vulnerability allows unauthenticated remote attackers to execute arbitrary code with the privileges of the SQL service account.

VU#484891 - Microsoft SQL Server 2000 contains stack buffer overflow in SQL Server Resolution Service

This vulnerability allows unauthenticated remote attackers to execute arbitrary code with the privileges of the SQL service account.

III. Solution

Apply a patch from Microsoft

VU#796313 - Microsoft SQL Server service account registry key has weak permissions that permit escalation of privileges

VU#225555 - Microsoft SQL Server contains buffer overflow in pwdencrypt() function

Microsoft has published Security Bulletin MS02-034 to address these vulnerabilities. For more information, please see

<http://www.microsoft.com/technet/security/bulletin/MS02-034.asp>

VU#627275 - Microsoft SQL Server extended stored procedures contain buffer overflows

Microsoft has published Security Bulletin MS02-020 to address this vulnerability. For more information, please see

<http://www.microsoft.com/technet/security/bulletin/MS02-020.asp>

VU#399260 - Microsoft SQL Server 2000 contains heap buffer overflow in SQL Server Resolution Service

VU#484891 - Microsoft SQL Server 2000 contains stack buffer overflow in SQL Server Resolution Service

Microsoft has published Security Bulletin MS02-039 to address these vulnerabilities. For more information, please see

<http://www.microsoft.com/technet/security/bulletin/MS02-039.asp>

Block external access to Microsoft SQL Server ports

As a workaround, it is possible to limit exposure to these vulnerabilities by restricting external access to Microsoft SQL Servers on ports 1433/tcp, 1433/udp, 1434/tcp, and 1434/udp. Note that VU#399260 and VU#484891 can be exploited using UDP packets with forged source addresses that appear to belong to legitimate services, so system administrators should restrict all incoming packets sent to 1434/udp.

Appendix A Vendor Information

This appendix contains information provided by vendors for this advisory. As vendors report new information to the CERT/CC, we will update this section and note the changes in our revision history. If a particular vendor is not listed below, we have not received their comments.

Appendix B CERT Vulnerability Notes sorted by Microsoft Security Bulletin ID

This appendix contains a list of CERT Vulnerability Notes sorted in reverse chronological order by their corresponding Microsoft Security Bulletin IDs. System administrators should use this list to ensure that each of the patches listed in these bulletins have been applied.

MS02-039 : Buffer Overruns in SQL Server 2000 Resolution Service Could Enable Code Execution (Q323875)

VU#399260 - Microsoft SQL Server 2000 contains heap buffer overflow in SQL Server Resolution Service

VU#484891 - Microsoft SQL Server 2000 contains stack buffer overflow in SQL Server Resolution Service

VU#370308 - Microsoft SQL Server 2000 contains denial-of-service vulnerability in SQL Server Resolution Service

MS02-038 : Unchecked Buffer in SQL Server 2000 Utilities Could Allow Code Execution (Q316333)

VU#279323 - Microsoft SQL Server contains buffer overflows in several Database Consistency Checkers

VU#508387 - Microsoft SQL Server contains SQL injection vulnerability in replication stored procedures

MS02-035 : SQL Server Installation Process May Leave Passwords on System (Q263968)

VU#338195 - Microsoft SQL Server installation process leaves sensitive information on system

MS02-034 : Cumulative Patch for SQL Server (Q316333)

VU#225555 - Microsoft SQL Server contains buffer overflow in `pwdencrypt()` function

VU#682620 - Microsoft SQL Server contains buffer overflow in code used to process "BULK INSERT" queries

VU#796313 - Microsoft SQL Server service account registry key has weak permissions that permit escalation of privileges

MS02-030 : Unchecked Buffer in SQLXML Could Lead to Code Execution (Q321911)

VU#811371 - Microsoft SQLXML ISAPI filter vulnerable to buffer overflow via *contenttype* parameter

VU#139931 - Microsoft SQLXML HTTP components vulnerable to cross-site scripting via *root* parameter

MS02-020 : SQL Extended Procedure Functions Contain Unchecked Buffers (Q319507)

VU#627275 - Microsoft SQL Server extended stored procedures contain buffer overflows

MS02-007 : SQL Server Remote Data Source Function Contain Unchecked Buffers

VU#619707 - Microsoft SQL Server contains buffer overflows in *openrowset* and *opendatasource*

macros

MS01-060 : SQL Server Text Formatting Functions Contain Unchecked Buffers

VU#700575 - Buffer overflows in Microsoft SQL Server 7.0 and SQL Server 2000

Appendix C References

<http://www.microsoft.com/technet/security/bulletin/MS02-007.asp>
<http://www.microsoft.com/technet/security/bulletin/MS02-020.asp>
<http://www.microsoft.com/technet/security/bulletin/MS02-030.asp>
<http://www.microsoft.com/technet/security/bulletin/MS02-034.asp>
<http://www.microsoft.com/technet/security/bulletin/MS02-035.asp>
<http://www.microsoft.com/technet/security/bulletin/MS02-038.asp>
<http://www.microsoft.com/technet/security/bulletin/MS02-039.asp>
<http://www.microsoft.com/technet/security/bulletin/MS01-060.asp>
<http://support.microsoft.com/support/misc/kblookup.asp?id=Q316333>
<http://support.microsoft.com/support/misc/kblookup.asp?id=Q319507>
<http://support.microsoft.com/support/misc/kblookup.asp?id=Q323875>
<http://www.microsoft.com/technet/security/MSDEapps.asp>
<http://www.microsoft.com/technet/prodtechnol/sql/maintain/security/sql2ksec.asp>
<http://www.appsecinc.com/resources/alerts/mssql/02-0000.html>
<http://www.nextgenss.com/vna/ms-sql.txt>
<http://www.theregister.co.uk/content/4/26086.html>
<http://www.securityfocus.com/bid/5014>
<http://www.securityfocus.com/bid/5204>
<http://www.securityfocus.com/bid/5205>
<http://www.kb.cert.org/vuls/id/139931>
<http://www.kb.cert.org/vuls/id/225555>
<http://www.kb.cert.org/vuls/id/279323>

<http://www.kb.cert.org/vuls/id/338195>

<http://www.kb.cert.org/vuls/id/370308>

<http://www.kb.cert.org/vuls/id/399260>

<http://www.kb.cert.org/vuls/id/484891>

<http://www.kb.cert.org/vuls/id/508387>

<http://www.kb.cert.org/vuls/id/619707>

<http://www.kb.cert.org/vuls/id/627275>

<http://www.kb.cert.org/vuls/id/682620>

<http://www.kb.cert.org/vuls/id/700575>

<http://www.kb.cert.org/vuls/id/796313>

<http://www.kb.cert.org/vuls/id/811371>

The CERT Coordination Center thanks NGSSoftware and Microsoft for their contributions to this document.

Author: This document was written by Jeffrey P. Lanza. Your feedback is appreciated.

Copyright 2002 Carnegie Mellon University

Revision History

Jul 29, 2002: Initial release

Jul 29, 2002: Updated impact section for VU#484891 and VU#399260

Feb 05, 2003: Updated systems affected and references sections to include URL for Microsoft list of MSDE applications

23 CA-2002-23: Multiple Vulnerabilities In OpenSSL

Original release date: July 30, 2002

Last revised: October 11, 2002

Source: CERT/CC

A complete revision history can be found at the end of this file.

Systems Affected

- OpenSSL prior to 0.9.6e, up to and including pre-release 0.9.7-beta2
- OpenSSL pre-release 0.9.7-beta2 and prior with Kerberos enabled
- SSLey library

Overview

There are four remotely exploitable buffer overflows in OpenSSL. There are also encoding problems in the ASN.1 library used by OpenSSL. Several of these vulnerabilities could be used by a remote attacker to execute arbitrary code on the target system. All could be used to create denial of service.

I. Description

OpenSSL is a widely deployed, open source implementation of the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) protocols as well as a full-strength general purpose cryptography library. The SSL and TLS protocols are used to provide a secure connection between a client and a server for higher level protocols such as HTTP. Four remotely exploitable vulnerabilities exist in many OpenSSL client and server systems.

VU#102795 - OpenSSL servers contain a buffer overflow during the SSLv2 handshake process

Versions of OpenSSL servers prior to 0.9.6e and pre-release version 0.9.7-beta2 contain a remotely exploitable buffer overflow vulnerability. This vulnerability can be exploited by a client using a malformed key during the handshake process with an SSL server connection. Note that only SSLv2-supported sessions are affected by this issue.

This issue is also being referenced as CAN-2002-0656.

VU#258555 - OpenSSL clients contain a buffer overflow during the SSLv3 handshake process

OpenSSL clients using SSLv3 prior to version 0.9.6e and pre-release version 0.9.7-beta2 contain a buffer overflow vulnerability. A malicious server can exploit this by sending a large session ID to the client during the handshake process.

This issue is also being referenced as CAN-2002-0656.

VU#561275 - OpenSSL servers with Kerberos enabled contain a remotely exploitable buffer overflow vulnerability during the SSLv3 handshake process

Servers running OpenSSL pre-release version 0.9.7 with Kerberos enabled contain a remotely exploitable buffer overflow vulnerability. This vulnerability can be exploited by a malicious client sending a malformed key during the SSLv3 handshake process with the server.

This issue is also being referenced as [CAN-2002-0657](#).

VU#308891 - OpenSSL contains multiple buffer overflows in buffers that are used to hold ASCII representations of integers

OpenSSL clients and servers prior to version 0.9.6e and pre-release version 0.9.7-beta2 contain multiple remotely exploitable buffer overflow vulnerabilities if running on 64-bit platforms. These buffers are used to hold ASCII representations of integers.

This issue is also being referenced as [CAN-2002-0655](#).

In addition, a separate issue has been identified in OpenSSL involving malformed ASN.1 encodings. Affected components include SSL or TLS applications, as well as S/MIME, PKCS#7, and certificate creation routines.

VU#748355 - ASN.1 encoding errors exist in implementations of SSL, TLS, S/MIME, PKCS#7 routines

The ASN.1 library used by OpenSSL has various encoding errors that allow malformed certificate encodings to be parsed incorrectly. Exploitation of this vulnerability can lead to remote denial-of-service issues. Routines affected include those supporting SSL and TLS applications, as well as those supporting S/MIME, PKCS#7, and certificate creation.

This issue is also being referenced as [CAN-2002-0659](#).

Although these vulnerabilities affect OpenSSL, other implementations of the SSL protocol that use or share a common code base may be affected. This includes implementations that are derived from the [SSLey library](#) developed by Eric A. Young and Tim J. Hudson.

As noted in the [OpenSSL advisory](#) as well, sites running OpenSSL 0.9.6d servers on 32-bit platforms with SSLv2 handshaking disabled will not be affected by any of the buffer overflows described above. However, due to the nature of the ASN.1 encoding errors, such sites may still be affected by denial-of-service situations.

II. Impact

By exploiting the buffer overflows above, a remote attacker can execute arbitrary code on a vulnerable server or client system or cause a denial-of-service situation. Exploitation of the ASN.1 encoding errors can lead to a denial of service.

III. Solution

Apply a patch from your vendor

Appendix A contains information provided by vendors for this advisory. As vendors report new information to the CERT/CC, we will update this section and note the changes in our revision history. If a particular vendor is not listed below or in the individual vulnerability notes, we have not received their comments. Please contact your vendor directly.

Upgrade to version 0.9.6e of OpenSSL

Upgrade to version 0.9.6e of OpenSSL to resolve the issues addressed in this advisory. As noted in the OpenSSL advisory, separate patches are available:

Combined patches for OpenSSL 0.9.6d:

http://www.openssl.org/news/patch_20020730_0_9_6d.txt

After either applying the patches above or upgrading to 0.9.6e, recompile all applications using OpenSSL to support SSL or TLS services, and restart said services or systems. This will eliminate all known vulnerable code.

Sites running OpenSSL pre-release version 0.9.7-beta2 may wish to upgrade to 0.9.7-beta3, which corrects these vulnerabilities. Separate patches are available as well:

Combined patches for OpenSSL 0.9.7 beta 2:

http://www.openssl.org/news/patch_20020730_0_9_7.txt

Disable vulnerable applications or services

Until fixes for these vulnerabilities can be applied, disable all applications that use vulnerable implementations of OpenSSL. Systems with OpenSSL 0.9.7 pre-release with Kerberos enabled also need to disable Kerberos to protect against VU#561275. As a best practice, the CERT/CC recommends disabling all services that are not explicitly required. Before deciding to disable SSL or TLS, carefully consider the impact that this will have on your service requirements.

Disabling SSLv2 handshaking will prevent exploitation of VU#102795. However, due to the nature of the ASN.1 encoding errors, such sites would still be vulnerable to denial-of-service attacks.

Appendix A Vendor Information

This appendix contains information provided by vendors for this advisory. As vendors report new information to the CERT/CC, we will update this section and note the changes in our revision history. If a particular vendor is not listed below or in the individual vulnerability notes, we have not received their comments.

Apple Computer, Inc.

The vulnerabilities described in this note are fixed with [Security Update 2002-08-02](#).

Alcatel

In relation to this CERT advisory on security vulnerability in OpenSSL, Alcatel has conducted an immediate assessment to determine any impact this may have on our portfolio. A first analysis has shown that various Alcatel products are affected: namely the 6600, 7700, 7800 and 8800 OmniSwitches, the OmniAccess 210 and the 7770 RCP. Alcatel is currently in the process of applying appropriate fixes to those products. Customers may contact their Alcatel support representative for more details. The security of our customers' networks is of highest priority for Alcatel. Therefore we continue to test our product portfolio against potential security vulnerabilities in our products using OpenSSL and will provide updates if necessary.

Covalent Technologies

Covalent Technologies has been informed by [RSA Security](#) that the BSAFE libraries used in Covalent's SSL implementations are potentially vulnerable to the SSL V2 negotiation issue detailed in [VU#102795](#) and the related [CA-2002-23](#) and [CA-2002-27](#) advisories. All Covalent products using SSL are affected. Covalent has product updates and additional information available at:

<http://www.covalent.net/products/rotate.php?page=110>

Debian Project

The Debian project has released [DSA 136](#) a while ago which fixes this vulnerability. Here's the link:

<http://www.debian.org/security/2002/dsa-136>

IBM

IBM's AIX operating system does not ship with OpenSSL; however, OpenSSL is available for installation on AIX via the Linux Affinity Toolkit. The version included on the Toolkit CD is vulnerable to the issues discussed here as well as the version of OpenSSL available for downloading from the IBM Linux Affinity website. Anyone running this version is advised to upgrade to the new version available from the website. This will be available within the next few days and can be downloaded from

<http://www6.software.ibm.com/dl/aixtbx/aixtbx-p>

This site contains Linux Affinity applications using cryptographic algorithms. New users to this site are asked to register first.

ISC

ISC Vendor statement.

BIND 4, BIND 8 and BIND 9.0.x are not vulnerable.

BIND 9.1.x ship with a copy of the vulnerable sections of OpenSSL crypto library (obj_dat.c and asn1_lib.c). Please upgrade to BIND 9.2.x and/or relink with a fixed version OpenSSL. e.g. configure --with-openssl=/path/to/fixed/openssl Vendors shipping product based on BIND 9.1 should contact bind-bugs@isc.org.

BIND 9.2.x is vulnerable if linked against a vulnerable library. By default BIND 9.2 does not link against OpenSSL.

Juniper Networks

Juniper has determined that our JUNOS Internet software (on M- and T-series routers) and the software running on our SDX and SSC products are potentially susceptible to the security vulnerabilities in OpenSSL. Corrected software images will be available for customer download shortly.

Software for our G10 CMTS product and our ERX products is unaffected by these vulnerabilities.

Lotus Software

Lotus products do not use OpenSSL or an SSLeay library, so they are not vulnerable. We further analyzed our SSL implementation for the issues reported in the advisory and determined that our products are not vulnerable.

Mandrake Software

Mandrake Linux update advisory MDKSA-2002:046-1 fixes all of these issues in OpenSSL. Please see

<http://www.mandrakesecure.net/en/advisories/2002/MDKSA-2002-046-1.php>

Microsoft Corporation

Microsoft products do not use the libraries in question. Microsoft products are not affected by this issue.

NetBSD

Please see [NetBSD-SA2002-009](#)

OpenLDAP

The [OpenLDAP Project](#) uses OpenSSL. Rebuilding OpenLDAP with updated versions of OpenSSL should adequately address reported issues. Those using packaged versions of OpenLDAP should contact the package distributor for update information.

OpenSSL

Please see http://www.openssl.org/news/secadv_20020730.txt.

Red Hat

Red Hat distributes affected versions of OpenSSL in all Red Hat Linux distributions as well as the Stronghold web server. Red Hat Linux errata packages that fix the above vulnerabilities ([CAN-2002-0655](#) and [CAN-2002-0656](#)) are available from the URL below. Users of the Red Hat Network are able to update their systems using the 'up2date' tool. A future update will fix the potential remote DOS in the ASN.1 encoding ([CAN-2002-0659](#))

<http://rhn.redhat.com/errata/RHSA-2002-155.html>

Secure Computing Corporation

In response to the CERT Advisory CA-2002-23, Secure Computing has posted a software patch for all users of the SafeWord PremierAccess version 3.1 authentication system. All existing and new customers are advised to download and apply PremierAccess Patch 1. Patch 1(3.1.0.01) is available for immediate web download at

<http://www.securecomputing.com/index.cfm?skey=1109>

These vulnerabilities were discovered and reported by the following:

- [VU#102795](#) - discovered by [A.L. Digital Ltd](#) and independently discovered and reported by John McDonald of Neohapsis
- [VU#258555](#), [VU#561275](#), [VU#308891](#) - discovered by [A.L. Digital Ltd](#)
- [VU#748355](#) - discovered by Adi Stav and James Yonan independently

The CERT/CC thanks the OpenSSL team for the work they put into their advisory, on which this document is largely based.

Feedback can be directed to the authors: [Jason A. Rafail](#), [Cory F. Cohen](#), [Jeffrey S. Havrilla](#), [Shawn V. Hernan](#).

Copyright 2002 Carnegie Mellon University

Revision History

July 30, 2002: Initial release

Aug 02, 2002: Added [IBM](#) statement from 07/31/2002

Aug 07, 2002: Added [NetBSD](#) statement from 08/01/2002

Aug 07, 2002: Added [Apple](#) statement from 08/02/2002

Aug 07, 2002: Added [Lotus](#) statement from 08/02/2002

Aug 07, 2002: Added [ISC](#) statement from 07/31/2002

Aug 15, 2002: Added [Juniper](#) statement from 08/15/2002

Sep 17, 2002: Added [Covalent](#) statement from 09/16/2002

Sep 20, 2002: Added Alcatel statement from 09/03/2002
Sep 23, 2002: Added Mandrake Software statement from 09/19/2002
Sep 26, 2002: Added Microsoft Corporation statement from 09/25/2002
Sep 30, 2002: Added Secure Computing Corporation statement from
09/24/2002
Oct 11, 2002: Added Debian statement from 10/08/2002

24 CA-2002-24: Trojan Horse OpenSSH Distribution

Original issue date: August 1, 2002

Last revised: August 2, 2002

Source: CERT/CC

A complete revision history is at the end of this file.

Overview

The CERT/CC has received confirmation that some copies of the source code for the OpenSSH package were modified by an intruder and contain a Trojan horse.

We strongly encourage sites which employ, redistribute, or mirror the OpenSSH package to immediately verify the integrity of their distribution.

I. Description

The CERT/CC has received confirmation that some copies of the source code for the OpenSSH package have been modified by an intruder and contain a Trojan horse. The following advisory has been released by the OpenSSH development team

<http://www.openssh.com/txt/trojan.adv>

The following files were modified to include the malicious code:

`openssh-3.4p1.tar.gz`

`openssh-3.4.tgz`

`openssh-3.2.2p1.tar.gz`

These files appear to have been placed on the FTP server which hosts `ftp.openssh.com` and `ftp.openbsd.org` on the 30th or 31st of July, 2002. The OpenSSH development team replaced the Trojan horse copies with the original, uncompromised versions at 13:00 UTC, August 1st, 2002. The Trojan horse copy of the source code was available long enough for copies to propagate to sites that mirror the OpenSSH site.

The Trojan horse versions of OpenSSH contain malicious code that is run when the software is compiled. This code connects to a fixed remote server on `6667/tcp`. It can then open a shell running as the user who compiled OpenSSH.

II. Impact

An intruder operating from (or able to impersonate) the remote address specified in the malicious code can gain unauthorized remote access to any host which compiled a version of OpenSSH

from this Trojan horse version of the source code. The level of access would be that of the user who compiled the source code.

III. Solution

We encourage sites who downloaded a copy of the OpenSSH distribution to verify the authenticity of their distribution, regardless of where it was obtained. Furthermore, we encourage users to inspect any and all software that may have been downloaded from the compromised site. Note that it is not sufficient to rely on the timestamps or sizes of the file when trying to determine whether or not you have a copy of the Trojan horse version.

Where to get OpenSSH

The primary distribution site for OpenSSH is

<http://www.openssh.com/>

Sites that mirror the OpenSSH source code are encouraged to verify the integrity of their sources.

Verify MD5 checksums

You can use the following MD5 checksums to verify the integrity of your OpenSSH source code distribution:

Correct versions:

```
459c1d0262e939d6432f193c7a4ba8a8 openssh-3.4p1.tar.gz
d5a956263287e7fd261528bb1962f24c openssh-3.4p1.tar.gz.sig
39659226ff5b0d16d0290b21f67c46f2 openssh-3.4.tgz
9d3e1e31e8d6cdbfa3036cb183aa4a01 openssh-3.2.2p1.tar.gz
be4f9ed8da1735efd770dc8fa2bb808a openssh-3.2.2p1.tar.gz.sig
```

At least one version of the modified Trojan horse distributions was reported to have the following checksum:

Trojan horse version:

```
3ac9bc346d736b4a51d676faa2a08a57 openssh-3.4p1.tar.gz
```

Verify PGP signature

Additionally, distributions of the portable release of OpenSSH are distributed with detached PGP signatures. Note that the Trojan horse versions were not signed correctly, and attempts to verify the signatures would have failed.

As a matter of good security practice, the CERT/CC encourages users to verify, whenever possible, the integrity of downloaded software. For more information, see

http://www.cert.org/incident_notes/IN-2001-06.html

Appendix A Vendor Information

This appendix contains information provided by vendors for this advisory. As vendors report new information to the CERT/CC, we will update this section and note the changes in our revision history. If a particular vendor is not listed below, we have not received their comments.

Connectiva Linux

Connectiva Linux distributes openssh-3.4p1 as a security update. The distributed copy is the original one and is not affected by this trojan. The detached digital signature is always checked before building third party packages.

Debian

Like one of our members, Matt Zimmerman, wrote earlier today:

```
pool/main/o/openssh/openssh_3.4p1.orig.tar.gz  
has md5sum 459c1d0262e939d6432f193c7a4ba8a8  
this refers to Debian GNU/Linux 3.0 (woody)
```

```
dists/potato/updates/main/source/openssh_3.4p1.orig.tar.gz  
has md5sum 459c1d0262e939d6432f193c7a4ba8a8  
this refers to Debian GNU/Linux 2.2 (potato)
```

```
security.debian.org/pool/updates/main/o/openssh/openssh_3.4p1.orig.tar.gz  
has md5sum 459c1d0262e939d6432f193c7a4ba8a8  
this refers to our security updates
```

all of which match the FreeBSD one, not the trojaned version.
They also match this signature:

```
ftp://ftp.openbsd.org/pub/OpenBSD/OpenSSH/portable/openssh-3.4p1.tar.gz.sig
```

from this key:

```
pub 1024D/86FF9C48 2001-02-26 Damien Miller (Personal Key) <djm@mindrot.org>  
Key fingerprint =3D 3981 992A 1523 ABA0 79DB FC66 CE8E CB03 86FF 9C48  
sub 2048g/AA2B1C41 2001-02-26
```

NetBSD

Both the OpenSSH in the base NetBSD system, and the OpenSSH distribution files available from ftp.netbsd.org have never been compromised with this trojan code.

NetBSD mirror sites retrieve their copy from ftp.netbsd.org, and so they would also be unaffected.

NetBSD pkgsrc compares downloaded distribution files against a known-good SHA1 hash to prevent the use of trojaned distribution files.

Nortel Networks

Nortel Networks products and solutions are not affected by the vulnerability identified in CERT Advisory CA-2002-24.

IBM Corporation

IBM's AIX operating system does not ship with OpenSSH; however, OpenSSH is available for installation on AIX via the Linux Affinity Toolkit. The packages currently available on the website do not contain the trojan code. We have verified that our OpenSSH packages were generated from clean source packages from the OpenSSH organization.

MandrakeSoft

MandrakeSoft has verified that the openssh-3.4p1 sources used to build its latest updates (ref. MDKSA-2002:040-1) do not contain this trojan.

Feedback can be directed to the author: [Chad Dougherty](#).

Copyright 2002 Carnegie Mellon University

Revision History

August 1, 2002: Initial release

August 1, 2002: Added IBM vendor statement

August 2, 2002: Added Debian, NetBSD, and Nortel vendor statements

25 CA-2002-25: Integer Overflow In XDR Library

Original release date: August 05, 2002

Last revised: October 03, 2002

Source: CERT/CC

A complete revision history can be found at the end of this file.

Systems Affected

Applications using vulnerable implementations of SunRPC-derived XDR libraries, which include, but are not limited to:

- Sun Microsystems network services library (libnsl)
- BSD-derived libraries with XDR/RPC routines (libc)
- GNU C library with sunrpc (glibc)

Overview

There is an integer overflow present in the `xdr_array()` function distributed as part of the Sun Microsystems XDR library. This overflow has been shown to lead to remotely exploitable buffer overflows in multiple applications, leading to the execution of arbitrary code. Although the library was originally distributed by Sun Microsystems, multiple vendors have included the vulnerable code in their own implementations.

I. Description

The XDR (external data representation) libraries are used to provide platform-independent methods for sending data from one system process to another, typically over a network connection. Such routines are commonly used in remote procedure call (RPC) implementations to provide transparency to application programmers who need to use common interfaces to interact with many different types of systems. The `xdr_array()` function in the XDR library provided by Sun Microsystems contains an integer overflow that can lead to improperly sized dynamic memory allocation. Subsequent problems like buffer overflows may result, depending on how and where the vulnerable `xdr_array()` function is used.

This issue is currently being tracked as VU#192995 by the CERT/CC and CAN-2002-0391 in the Common Vulnerabilities and Exposures (CVE) dictionary.

II. Impact

Because SunRPC-derived XDR libraries are used by a variety of vendors in a variety of applications, this defect may lead to a number of differing security problems. Exploiting this vulnerability will lead to denial of service, execution of arbitrary code, or the disclosure of sensitive information.

Specific impacts reported include the ability to execute arbitrary code with root privileges (by exploiting [dmispd](#), [rpc.cmsd](#), or [kadmind](#), for example). In addition, intruders who exploit the XDR overflow in [MIT KRB5](#) kadmind may be able to gain control of a Key Distribution Center (KDC) and improperly authenticate to other services within a trusted Kerberos realm.

III. Solution

Apply a patch from your vendor

[Appendix A](#) contains information provided by vendors for this advisory. As vendors report new information to the CERT/CC, we will update this section and note the changes in our revision history. If a particular vendor is not listed below or in the [vulnerability note](#), we have not received their comments. Please contact your vendor directly.

Note that XDR libraries can be used by multiple applications on most systems. It may be necessary to upgrade or apply multiple patches and then recompile statically linked applications.

Applications that are statically linked must be recompiled using patched libraries. Applications that are dynamically linked do not need to be recompiled; however, running services need to be restarted in order to use the patched libraries.

System administrators should consider the following process when addressing this issue:

1. Patch or obtain updated XDR/RPC libraries.
2. Restart any dynamically linked services that make use of the XDR/RPC libraries.
3. Recompile any statically linked applications using the patched or updated XDR/RPC libraries.

Disable access to vulnerable services or applications

Until patches are available and can be applied, you may wish to disable access to services or applications compiled with the vulnerable `xdr_array()` function. Such applications include, but are not limited to, the following:

- DMI Service Provider daemon (`dmispd`)
- CDE Calendar Manager Service daemon (`rpc.cmsd`)
- MIT Kerberos 5 Administration daemon (`kadmind`)

As a best practice, the CERT/CC recommends disabling all services that are not explicitly required.

Appendix A Vendor Information

This appendix contains information provided by vendors for this advisory. As vendors report new information to the CERT/CC, we will update this section and note the changes in our revision history. If a particular vendor is not listed below or in the individual [vulnerability notes](#), we have not received their comments.

Apple Computer, Inc.

The vulnerability described in this note is fixed with [Security Update 2002-08-02](#).

Debian GNU/Linux

The Debian GNU/Linux distribution was vulnerable with regard to the the XDR problem as stated above with the following vulnerability matrix:

	OpenAFS	Kerberos5	GNU libc
Debian 2.2 (potato)	not included	not included	vulnerable
Debian 3.0 (woody)	vulnerable (DSA 142-1)	vulnerable (DSA 143-1)	vulnerable
Debian unstable (sid)	vulnerable (DSA 142-1)	vulnerable (DSA 143-1)	vulnerable

However, the following advisories were raised recently which contain and announced fixes:

[DSA 142-1 OpenAFS](#) (safe version are: 1.2.3final2-6 (woody) and 1.2.6-1 (sid))

[DSA 143-1 Kerberos5](#) (safe version are: 1.2.4-5woody1 (woody) and 1.2.5-2 (sid))

The advisory for the GNU libc is pending, it is currently being recompiled. The fixed versions will probably be:

Debian 2.2 (potato) glibc 2.1.3-23 or later

Debian 3.0 (woody) glibc 2.2.5-11.1 or later

Debian unstable (sid) glibc 2.2.5-12 or later

GNU glibc

Version 2.2.5 and earlier versions of the GNU C Library are vulnerable. For Version 2.2.5, we suggest the following patch. This patch is also available from the GNU C Library CVS repository at:

http://sources.redhat.com/cgi-bin/cvsweb.cgi/libc/sunrpc/xdr_ar-ray.c.diff?r1=1.5&r2=1.5.2.1&cvsroot=glibc

2002-08-02 Jakub Jelinek <jakub@redhat.com>

- sunrpc/xdr_array.c (xdr_array): Check for overflow on multiplication. Patch by Solar Designer <solar@openwall.com>.

[text of diff available in [CVS repository](#) link above --CERT/CC]

FreeBSD, Inc.

Please see <ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-02:34.rpc.asc>

Hewlett-Packard Company

SOURCE: Hewlett-Packard Company

RE: Potential RPC XDR buffer overflow

At the time of writing this document, Hewlett Packard is currently investigating the potential impact to HP's released operating System software products.

As further information becomes available HP will provide notice of the availability of any necessary patches through standard security bulletin announcements and be available from your normal HP Services support channel.

IBM Corporation

IBM is vulnerable to the above XDR Library issues in both the 4.3 and 5.1 releases of AIX. A temporary patch is currently available through an efix package. Efixes are available from

<ftp.software.ibm.com/aix/efixes/security/>

See the [README](#) file in this directory for additional information on the efixes.

The following APARs will be available in the near future:

AIX 4.3.3: APAR #IY34194 (available approx 10/1/2002)

AIX 5.1.0: APAR #IY34158 (available approx 10/16/2002)

Juniper Networks

The Juniper Networks SDX-300 Service Deployment System (SSC) does use XDR for communication with an ERX edge router, but does not make use of the Sun RPC libraries. The SDX-300 product is not vulnerable to the Sun RPC XDR buffer overflow as outlined in this CERT advisory.

KTH and Heimdal Kerberos

kth-krb and heimdal are not vulnerable to this problem since they do not use any Sun RPC at all.

MIT Kerberos Development Team

Please see <http://web.mit.edu/kerberos/www/advisories/MITKRB5-SA-2002-001-xdr.txt>

The patch is available directly:

http://web.mit.edu/kerberos/www/advisories/2002-001-xdr_array_patch.txt

The following detached PGP signature should be used to verify the authenticity and integrity of the patch:

http://web.mit.edu/kerberos/www/advisories/2002-001-xdr_array_patch.txt.asc

Microsoft Corporation

Microsoft is currently conducting an investigation based on this report. We will update this advisory with information once it is complete.

NetBSD

Please see <ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2002-011.txt.asc>

Network Appliance

NetApp systems are not vulnerable to this problem.

OpenAFS

OpenAFS is an affected vendor for this vulnerability. <http://www.openafs.org/pages/security/OPENAFS-SA-2002-001.txt> details how we have dealt with the issue.

Openwall Project

The *xdr_array(3)* integer overflow was present in the glibc package on Openwall GNU*/Linux until 2002/08/01 when it was corrected for Owl-current and documented as a security fix in the system-wide change log available at:

<http://www.openwall.com/Owl/CHANGES.shtml>

The same glibc package update also fixes a very similar but different *calloc(3)* integer overflow possibility that is currently not known to allow for an attack on a particular application, but has been patched as a proactive measure. The Sun RPC *xdr_array(3)* overflow may allow for passive attacks on *mount(8)* by malicious or spoofed NFSv3 servers as well as for both passive and active attacks on RPC clients or services that one might install on Owl. (There're no RPC services included with Owl.)

RedHat Inc.

Red Hat distributes affected packages glibc and Kerberos in all Red Hat Linux distributions. We are currently working on producing errata packages, when complete these will be available along

with our advisory at the URLs below. At the same time users of the Red Hat Network will be able to update their systems using the 'up2date' tool.

<http://rhn.redhat.com/errata/RHSA-2002-166.html> (glibc)

<http://rhn.redhat.com/errata/RHSA-2002-172.html> (Kerberos 5)

SGI

SGI now has patches available to fix this problem, per 20020801-01-P:

<ftp://patches.sgi.com/support/free/security/advisories/20020801-01-P>

Sun Microsystems, Inc.

Sun can confirm that there is a type overflow vulnerability in the *xdr_array(3NSL)* function which is part of the network services library, *libnsl(3LIB)*, on Solaris 2.5.1 through 9. Sun has published Sun Alert 46122 which describes the issue, applications affected, and workaround information. The Sun Alert will be updated as more information or patches become available and is located here:

<http://sunsolve.Sun.COM/pub-cgi/retrieve.pl?doc=fsalert%2F46122>

Sun will be publishing a Sun Security Bulletin for this issue once all of the patches are available which will be located at:

<http://sunsolve.sun.com/security>

Appendix B References

1. Manual entry for xdr_array(3)
2. VU#192995
3. RFC1831
4. RFC1832
5. Sun Alert 46122
6. Security Alert MITKRB5-SA-2002-001-xdr
7. Flaw in calloc and similar routines, Florian Weimer, University of Stuttgart, RUS-CERT, 2002-08-05
8. MS02-057: Flaw in Services for Unix 3.0 Interix SDK Could Allow Code Execution (Q329209)

Thanks to Sun Microsystems for working with the CERT/CC to make this document possible. The initial vulnerability research and demonstration was performed by Internet Security Systems (ISS).

Authors: Jeffrey S. Havrilla and Cory F. Cohen

Copyright 2002 Carnegie Mellon University

Revision History

Aug 05, 2002: Initial release

Aug 06, 2002: Minor update to Debian statement, corrected glibc for Debian 3.0 (woody) will be 2.2.5-11.1 or later

Aug 06, 2002: Added IBM statement

Aug 19, 2002: Updated SGI statement

Sep 03, 2002: Updated IBM statement

Oct 03, 2002: Added Microsoft Bulletin MS02-057 to list of references

26 CA-2002-26: Buffer Overflow in CDE ToolTalk

Original release date: August 12, 2002

Last revised: September 9, 2002

Source: CERT/CC

A complete revision history can be found at the end of this file.

Systems Affected

- Systems running CDE ToolTalk

Overview

The Common Desktop Environment (CDE) ToolTalk RPC database server contains a buffer overflow vulnerability that could allow a remote attacker to execute arbitrary code or cause a denial of service.

I. Description

The Common Desktop Environment (CDE) is an integrated graphical user interface that runs on UNIX and Linux operating systems. CDE ToolTalk is a message brokering system that provides an architecture for applications to communicate with each other across hosts and platforms. The ToolTalk RPC database server, `rpc.ttdbserverd`, manages communication between ToolTalk applications. For more information about CDE, see

<http://www.opengroup.org/cde/>

<http://www.opengroup.org/desktop/faq/>

The CDE ToolTalk database server is vulnerable to a heap buffer overflow via an argument passed to the procedure `_TT_CREATE_FILE()`. An attacker with access to the ToolTalk RPC database service could exploit this vulnerability with a specially crafted RPC message.

Vulnerability Note [VU#387387](#) includes a list of vendors who have been contacted about this vulnerability.

This vulnerability was discovered and reported by the Entercept Ricochet Team and is described in the following Entercept Security Alert:

<http://www.entercept.com/news/uspr/08-12-02.asp>

This vulnerability has been assigned [CAN-2002-0679](#) by the Common Vulnerabilities and Exposures (CVE) group.

A list previously documented problems in CDE can be found in [Appendix B](#).

II. Impact

Using an RPC message containing a specially crafted argument to `_TT_CREATE_FILE()`, a remote attacker could execute arbitrary code or cause a denial of service. The ToolTalk database server process runs with root privileges on most systems. Note that the non-executable stack protection provided by some operating systems will not prevent the execution of code located on the heap.

III. Solution

Apply a patch from your vendor

[Appendix A](#) contains information provided by vendors for this advisory. As vendors report new information to the CERT/CC, we will update this section and note the changes in our revision history. If a particular vendor is not listed below, we have not received their comments. Please contact your vendor directly.

Disable vulnerable service

Until patches are available and can be applied, you may wish to disable the ToolTalk RPC database service. As a best practice, the CERT/CC recommends disabling all services that are not explicitly required. On a typical CDE system, it should be possible to disable `rpc.ttdbserverd` by commenting out the relevant entries in `/etc/inetd.conf` and if necessary, `/etc/rpc`, and then by restarting the `inetd` process.

The program number for the ToolTalk RPC database server is 100083. If references to 100083 or `rpc.ttdbserverd` appear in `/etc/inetd.conf` or `/etc/rpc` or in output from the `rpcinfo(1M)` and `ps(1)` commands, then the ToolTalk RPC database server may be running.

The following example was taken from a system running SunOS 5.8 (Solaris 8):

```
/etc/inetd.conf
...
#
# Sun ToolTalk Database Server
#
100083/1 tli rpc/tcp wait root /usr/dt/bin/rpc.ttdbserverd rpc.ttdb-
serverd
...
# rpcinfo -p
program vers proto port service
...
100083 1 tcp 32773
...
```

```
# ps -ef
UID PID PPID C STIME TTY TIME CMD
...
root 355 164 0 19:31:27 ? 0:00 rpc.ttdbserverd
...
```

Before deciding to disable the ToolTalk RPC database server or the RPC portmapper service, carefully consider your network configuration and service requirements.

Block access to vulnerable service

Until patches are available and can be applied, you may wish to block access to the ToolTalk RPC database server and possibly the RPC portmapper service from untrusted networks such as the Internet. Use a firewall or other packet-filtering technology to block the appropriate network ports. The ToolTalk RPC database server may be configured to use port 692/tcp or another port as indicated in output from the `rpcinfo(1M)` command. In the example above, the ToolTalk RPC database server is configured to use port 32773/tcp. The RPC portmapper service typically runs on ports 111/tcp and 111/udp. Keep in mind that blocking ports at a network perimeter does not protect the vulnerable service from attacks that originate from the internal network.

Before deciding to block or restrict access to the ToolTalk RPC database server or the RPC portmapper service, carefully consider your network configuration and service requirements.

Appendix A Vendor Information

This appendix contains information provided by vendors for this advisory. As vendors report new information to the CERT/CC, we will update this section and note the changes in our revision history. If a particular vendor is not listed below, we have not received their comments.

Caldera, Inc.

Caldera Open UNIX and Caldera UnixWare provide the CDE `ttdbserverd` daemon, and are vulnerable to these issues. Please see Caldera Security Advisory [CSSA-2002-SCO.28.1](#) for more information.

SCO OpenServer and Caldera OpenLinux do not provide CDE, and are therefore not vulnerable.

Cray, Inc.

Cray, Inc. does include ToolTalk within the CrayTools product. However, `rpc.ttdbserverd` is not turned on or used by any Cray provided application. Since a site may have turned this on for their own use, they can always remove the binary `/opt/ctl/bin/rpc.ttdbserverd` if they are concerned.

Hewlett-Packard Company

SOURCE: Hewlett-Packard Company Software Security Response Team (SSRT)

Date: 15 August, 2002

CROSS REFERENCE ID: SSRT2274

HP Tru64 UNIX

[Hewlett-Packard has released a security bulletin ([SRB0039W/SSRT2274](#)) that addresses VU#387387 and other vulnerabilities.]

HP-UX

A preliminary fix for HP-UX is available:

Originally issued: 12 July 2002

Last revision: 14 Aug 2002

<ftp://ttdb1:ttdb1@hprc.external.hp.com/>

file: rpc.ttdbserver.2.tar.gz

Details can be found in HPSBUX0207-199 at <http://itrc.hp.com>

NOT IMPACTED:

HP-MPE/ix

HP OpenVMS

HP NonStop Servers

HP Recommended Workaround:

A recommended workaround is to disable `rpc.ttdbserverd` until solutions are available. This should only create a potential problem for public software packages applications that use the RPC-based ToolTalk database server. This step should be evaluated against the risks identified, your security measures environment, and potential impact of other products that may use the ToolTalk database server.

To disable `rpc.ttdbserverd`:

HP Tru64 Unix:

Comment out the following line in `/etc/inetd.conf`:

```
rpc.ttdbserverd stream tcp swait root /usr/dt/bin/rpc.ttdbserverd
rpc.ttdbserverd
```

Force `inetd` to re-read the configuration file by executing the `inetd -h` command.

Note: The internet daemon should kill the currently running `rpc.ttdbserver`. If not, manually kill any existing `rpc.ttdbserverd` process.

HP-UX:

Comment out the following line in `/etc/inetd.conf`:

```
rpc stream tcp swait root /usr/dt/bin/rpc.ttdbserver 100083 1
/usr/dt/bin/rpc.ttdbserver [10.20]
```

or

```
rpc xti tcp swait root /usr/dt/bin/rpc.ttdbserver 100083 1
/usr/dt/bin/rpc.ttdbserver [11.0/11.11]
```

Force `inetd` to re-read the configuration file by executing the `inetd -c` command.

Note: The internet daemon should kill the currently running `rpc.ttdbserver`. If not, manually kill any existing `rpc.ttdbserverd` process.

To report potential security vulnerabilities in HP software, send an E-mail message to: security-alert@hp.com

IBM Corporation

The CDE desktop product shipped with AIX is vulnerable to the issue detailed above in the advisory. This affects AIX releases 4.3.3 and 5.1.0. An efix package for this issue is currently available from the IBM software ftp site.

The efix packages can be downloaded via anonymous ftp from [ftp.software.ibm.com/aix/efixes/security/](ftp://ftp.software.ibm.com/aix/efixes/security/). This directory contains a README file that gives further details on the efix packages.

The following APARs will be available in the near future:

AIX 4.3.3: IY32792

AIX 5.1.0: IY32793

SGI

SGI acknowledges the ToolTalk vulnerabilities reported by CERT and is currently investigating. No further information is available at this time.

For the protection of all our customers, SGI does not disclose, discuss or confirm vulnerabilities until a full investigation has occurred and any necessary patch(es) or release streams are available for all vulnerable and supported IRIX operating systems. Until SGI has more definitive information to provide, customers are encouraged to assume all security vulnerabilities as exploitable and take appropriate steps according to local site security policies and requirements. As further information becomes available, additional advisories will be issued via the normal SGI security information distribution methods including the wiretap mailing list on <http://www.sgi.com/support/security/>.

Sun Microsystems, Inc.

The Solaris RPC-based ToolTalk database server, `rpc.ttdbserverd`, is vulnerable to the buffer overflow described in this advisory in all currently supported versions of Solaris:

Solaris 2.5.1, 2.6, 7, 8, and 9

Patches are being generated for all of the above releases. Sun will be publishing Sun Alert 46366 for this issue which will be located here:

<http://sunsolve.Sun.COM/pub-cgi/retrieve.pl?doc=fsalert%2F46366>

The Sun Alert will be updated as more information or patches become available. The patches will be available from:

<http://sunsolve.sun.com/securitypatch>

Sun will be publishing a Sun Security Bulletin for this issue once all of the patches are available which will be located at:

<http://sunsolve.sun.com/security>

Xi Graphics

Xi Graphics deXtop CDE v2.1 is vulnerable to this attack. The update and accompanying text file will be:

<ftp://ftp.xig.com/pub/updates/dextop/2.1/DEX2100.016.tar.gz>

<ftp://ftp.xig.com/pub/updates/dextop/2.1/DEX2100.016.txt>

DeXtop version 3.0 already contains this fix.

Most sites do not need to use the ToolTalk server daemon. Xi Graphics Security recommends that non-essential services are never enabled. To disable the ToolTalk server on your system, edit `/etc/inetd.conf` and comment out, or remove, the `'rpc.ttdbserver'` line. Then, either restart `inetd`, or reboot your machine.

Appendix B References

- <http://www.opengroup.org/cde/>
- <http://www.opengroup.org/desktop/faq/>
- <http://www.entercept.com/news/uspr/08-12-02.asp>
- <http://www.cert.org/advisories/CA-2002-20.html>
- <http://www.kb.cert.org/vuls/id/975403>
- <http://www.kb.cert.org/vuls/id/299816>
- <http://www.cert.org/advisories/CA-2002-01.html>
- <http://www.cert.org/advisories/CA-2001-31.html>
- <http://www.kb.cert.org/vuls/id/172583>

- <http://www.cert.org/advisories/CA-2001-27.html>
- <http://www.kb.cert.org/vuls/id/595507>
- <http://www.kb.cert.org/vuls/id/860296>
- <http://www.cert.org/advisories/CA-1999-11.html>
- <http://www.cert.org/advisories/CA-1998-11.html>
- <http://www.cert.org/advisories/CA-1998-02.html>

The CERT Coordination Center thanks Sinan Eren of the Entercept Richochet Team for reporting this vulnerability.

Author: Art Manion

Copyright 2002 Carnegie Mellon University

Revision History

August 12, 2002: Initial release

August 13, 2002: Updated IBM statement

August 15, 2002: Updated HP statement

August 20, 2002: Updated Caldera and HP statements

September 9, 2002: Updated HP statement

27 CA-2002-27: Apache/mod_ssl Worm

Original release date: September 14, 2002

Last revised: October 11, 2002

Source: CERT/CC

A complete revision history can be found at the end of this file.

Systems Affected

- Linux systems running Apache with mod_ssl accessing SSLv2-enabled OpenSSL 0.9.6d or earlier on Intel x86 architectures

Overview

The CERT/CC has received reports of self-propagating malicious code which exploits a vulnerability ([VU#102795](#)) in OpenSSL. This malicious code has been referred to as Apache/mod_ssl worm, linux.slapper.worm and bugtraq.c worm. Reports received by the CERT/CC indicate that the Apache/mod_ssl worm has already infected thousands of systems. There are currently at least three known variants of this worm in circulation.

I. Description

The Apache/mod_ssl worm is self-propagating malicious code that exploits the OpenSSL vulnerability described in [VU#102795](#). This vulnerability was the among the topics discussed in [CA-2002-23 Multiple Vulnerabilities In OpenSSL](#). While this OpenSSL server vulnerability exists on a wide variety of platforms, the Apache/mod_ssl worm appears to work only on Linux systems running Apache with the OpenSSL module (mod_ssl) on Intel architectures.

The Apache/mod_ssl worm scans for potentially vulnerable systems on 80/tcp using an invalid HTTP GET request. When a potentially vulnerable Apache system is detected, the worm attempts to connect to the SSL service via 443/tcp in order to deliver the exploit code. If successful, a copy of the malicious source code is then placed on the victim server, where the attacking system tries to compile and run it. Once infected, the victim server begins scanning for additional hosts to continue the worm's propagation.

Additionally, the Apache/mod_ssl worm can act as an attack platform for distributed denial-of-service (DDoS) attacks against other sites by building a network of infected hosts. During the infection process, the attacking host instructs the newly-infected victim to initiate traffic on 2002/udp (newer variants have been reported using 1978/udp or 4156/udp) back to the attacker. Once this communications channel has been established, the infected system becomes part of the Apache/mod_ssl worm's DDoS network. Infected hosts can then share information on other infected systems as well as attack instructions. Thus, this UDP traffic can be used by a remote attacker as a communications channel between infected systems to coordinate attacks on other sites.

Reports to the CERT/CC indicate that the high volume of 1978/udp, 2002/udp, or 4156/udp traffic generated between hosts infected with the Apache/mod_ssl worm may itself lead to performance issues (including possible denial-of-service conditions) on networks with infected hosts. Furthermore, since repairing an infected host does not remove its IP address from the Apache/mod_ssl worm's Peer-to-Peer network, sites that have had hosts infected with the Apache/mod_ssl worm and subsequently patched them may continue to see significant levels of 1978/udp, 2002/udp, or 4156/udp traffic directed at those formerly infected systems.

Identifying infected hosts

During the infection process of the "A" variant of the Apache/mod_ssl worm, an encoded version of the worm's source code is placed in `/tmp/.uubugtraq`. This file is then decoded into `/tmp/.bugtraq.c`, compiled with `gcc`, and the executable binary is subsequently stored at `/tmp/.bugtraq`. More recent variants follow a similar (but not identical) pattern of infection, and leave behind different files. Because all three variants exploit the same system vulnerabilities, it is possible that systems infected with one variant may also become infected with the others. Therefore, presence of any of the following files on Linux systems running Apache with OpenSSL is indicative of compromise.

Variant "A"

`/tmp/.uubugtraq`

`/tmp/.bugtraq.c`

`/tmp/.bugtraq`

Variant "B"

`/tmp/.unlock.c`

`/tmp/.update.c`

Variant "C"

`/tmp/.cinik`

`/tmp/.cinik.c`

`/tmp/.cinik.go`

`/tmp/.cinik.goecho`

`/tmp/.cinik.uu`

The probing phase of the attack may show up in web server log as shown in the example below. It is important to note that there may be other causes of such log entries, so the appearance of entries matching (or similar to) these in a web server log should **not** be construed as evidence of compromise. Rather, their presence is indicative that further investigation may be warranted.

Example: Initial probe to identify web server software version

```
GET / HTTP/1.1
```

Note: Based on initial reports received by the CERT/CC, earlier versions of this Advisory mentioned other SSL error messages that might be logged on potentially vulnerable hosts. On further analysis, we have concluded that these log messages were unrelated to the the Apache/mod_ssl worm. An explanation of one possible cause of those other mod_ssl error messages was provided by Inktomi and appears in Appendix A below.

Hosts found to be listening for or transmitting data on 1978/udp (variant "C"), 2002/udp (variant "A"), or 4156/udp (variant "B") are also indicative of compromise by the Apache/mod_ssl worm.

In addition to communicating with other infected hosts via 4156/udp, the "B" variant of the Apache/mod_ssl worm creates a backdoor listening on 1052/tcp.

Detecting Apache/mod_ssl worm activity on the network

Infected systems are readily identifiable on a network by the following traffic characteristics:

- Probing -- Scanning on 80/tcp
- Propagation -- Connections to 443/tcp
- DDoS -- Transmitting or receiving datagrams with both source and destination ports 1978/udp, 2002/udp, or 4156/udp. This traffic is used as a communications channel between infected systems to coordinate attacks on other sites.
- Backdoor ("B" variant only) -- Listening on 1052/tcp.

Additionally, infected hosts that are actively participating in DDoS attacks against other systems may generate unusually high volumes of attack traffic using various protocols (e.g., TCP, UDP, ICMP)

II. Impact

Compromise by the Apache/mod_ssl worm indicates that a remote attacker can execute arbitrary code as the apache user on the victim system. It may be possible for an attacker to subsequently leverage a local privilege escalation exploit in order to gain root access to the victim system. The high volume of 2002/udp traffic (1978/udp or 4156/udp in newer variants) generated between hosts infected with the Apache/mod_ssl worm may itself lead to performance issues on networks with infected or formerly infected hosts. Furthermore, the DDoS capabilities included in the Apache/mod_ssl worm allow victim systems to be used as platforms to attack other systems.

III. Solution

Apply a patch

Administrators of all systems running OpenSSL are encouraged to review [CA-2002-23](#) and [VU#102795](#) for detailed vendor recommendations regarding patches. Additional vendor information is available in [Appendix A](#) below.

Note that while the vulnerability exploited by the Apache/mod_ssl worm was fixed beginning with OpenSSL version [0.9.6e](#), as of this writing the latest version of OpenSSL is [0.9.6g](#). Administrators may wish to upgrade to that version instead.

The following is reproduced in part from [CA-2002-23](#)

Upgrade to version 0.9.6e of OpenSSL

Upgrade to version [0.9.6e](#) of OpenSSL to resolve the issues addressed in this advisory. As noted in the [OpenSSL advisory](#), separate patches are available:

Combined patches for OpenSSL 0.9.6d:

http://www.openssl.org/news/patch_20020730_0_9_6d.txt

After either applying the patches above or upgrading to [0.9.6e](#), recompile all applications using OpenSSL to support SSL or TLS services, and restart said services or systems. This will eliminate all known vulnerable code.

Sites running OpenSSL pre-release version 0.9.7-beta2 may wish to upgrade to [0.9.7-beta3](#), which corrects these vulnerabilities. Separate patches are available as well:

Combined patches for OpenSSL 0.9.7 beta 2:

http://www.openssl.org/news/patch_20020730_0_9_7.txt

Disable SSLv2

Disabling SSLv2 handshaking will prevent exploitation of [VU#102795](#). CERT/CC recommends consulting the mod_ssl documentation for a complete description of the options but one method for disabling SSLv2 is to remove SSLv2 as a supported cipher in the `SSLCipherSuite` directive in the configuration file. For example:

```
SSLCipherSuite ALL:!ADH:RC4+RSA:+HIGH:+SSLv2
```

which allows SSLv2 can be changed to

```
SSLCipherSuite ALL:!ADH:RC4+RSA:+HIGH:!SSLv2
```

which will disable SSLv2. Note the changing of `+SSLv2` to `!SSLv2`.

However, systems may still be susceptible to the other vulnerabilities described in [CA-2002-23](#).

Ingress/Egress filtering

The following steps are only effective in limiting the damage that systems already infected with the Apache/mod_ssl worm can do. They provide no protection whatsoever against the initial infection of systems. As a result, these steps are only recommended **in addition to** the preventative steps outlined above, not in lieu thereof.

Ingress filtering manages the flow of traffic as it enters a network under your administrative control. Servers are typically the only machines that need to accept inbound traffic from the public Internet. In the network usage policy of many sites, external hosts are only permitted to initiate inbound traffic to machines that provide public services on specific ports. Thus, ingress filtering should be performed at the border to prohibit externally initiated inbound traffic to non-authorized services.

Egress filtering manages the flow of traffic as it leaves a network under your administrative control. There is typically limited need for machines providing public services to initiate outbound connections to the Internet.

In the case of the Apache/mod_ssl worm, employing ingress and egress filtering can help prevent systems on your network from participating in the worm's DDoS network and attacking systems elsewhere. Blocking UDP datagrams with both source and destination ports 1978, 2002 and 4156 from entering or leaving your network reduces the risk of external infected systems communicating with infected hosts inside your network.

Recovering from a system compromise

If you believe a system under your administrative control has been compromised, please follow the steps outlined in

[Steps for Recovering from a UNIX or NT System Compromise](#)

Reporting

The CERT/CC is interested in receiving reports of this activity. If machines under your administrative control are compromised, please send mail to cert@cert.org with the following text included in the subject line: "[CERT#23820]".

Appendix A Vendor Information

This appendix contains information provided by vendors for this advisory. As vendors report new information to the CERT/CC, we will update this section and note the changes in our revision history. If a particular vendor is not listed below, we have not received their comments.

Apple Computer, Inc.

The vulnerability described in this report has been addressed by

- [Security Update 2002-08-23](#) for Mac OS X 10.2 (Jaguar), and by
- [Security Update 2002-08-02](#) for Mac OS X 10.1.5.

Covalent Technologies

Covalent Technologies has been informed by RSA Security that the BSAFE libraries used in Covalent's SSL implementations are potentially vulnerable to the SSL V2 negotiation issue detailed in VU 102795 and the related CA-2002-23 and CA-2002-27 advisories. All Covalent products using SSL are affected. Covalent has product updates and additional information available at: <http://www.covalent.net/products/rotate.php?page=110>

Debian Project

The Debian project has released [DSA 136](#) a while ago which fixes this vulnerability. Here's the link: <http://www.debian.org/security/2002/dsa-136>

Inktomi

As noted in the advisory, server log messages such as

```
GET /mod_ssl:error:HTTP-request HTTP/1.0
```

do not necessarily indicate access by a compromised system. Any HTTP request to a port expecting to serve HTTPS requests will generate this log message. The Inktomi web crawler follows URL links published on public web pages and is sometimes incorrectly directed to https servers. The crawler does not use Apache nor mod_ssl (nor any kind of SSL), so it is not subject to the compromise described in this advisory. But crawler requests can match two of the listed symptoms of the Apache/mod_ssl worm:

- Probing -- Scanning on 80/tcp
- Propagation -- Connections to 443/tcp

The crawler does not use port 2002 nor UDP. Port 80 access or HTTPS handshake errors from an Inktomi web crawler do not represent an attack on your web server.

Inktomi crawler systems have hostnames of the form

```
j[1-9][0-9][0-9][0-9].inktomisearch.com  
si[1-9][0-9][0-9][0-9].inktomisearch.com
```

The IP addresses of Inktomi crawler hosts will reverse-DNS resolve to a name of this form.

Red Hat Inc.

Versions of OpenSSL that are not vulnerable to this issue have been available from Red Hat since 29th July 2002. Customers who have kept their systems up to date by applying fixes or using the Red Hat Network are not impacted by this worm. Updates for all affected Red Hat products are available; details and links to the individual advisories can be found at

http://www.redhat.com/support/alerts/linux_slapper_worm.html

Feedback can be directed to the author: [Allen Householder](#).

Copyright 2002 Carnegie Mellon University

Revision History

September 14, 2002: Initial release

September 16, 2002: Updated details on 2002/udp traffic in Description, Impact sections

September 16, 2002: Clarified example web server log entries in Description section

September 16, 2002: Added Ingress/Egress filtering section to Solutions section

September 17, 2002: Clarified example log entries seen by probed servers

September 17, 2002: Added [Apple](#) vendor statement made 9/16/2002 1:48:09 PM (UTC-0700)

September 17, 2002: Removed references to "GET /mod_ssl:error:HTTP-request" appearing in server logs

September 17, 2002: Added [Inktomi](#) vendor statement made 9/16/2002 09:16:09 AM (UTC-0700)

September 17, 2002: Added [Covalent Technologies](#) vendor statement made 9/16/2002 09:59:00 AM (UTC-0700)

September 19, 2002: Added [Red Hat Inc.](#) vendor statement made 2002-09-18 09:44:14 (UTC+0100)

September 23, 2002: Added mention of 1978/udp and 4156/udp in use by newer variants of the worm

September 23, 2002: Added additional details on the "B" and "C" variants of the worm.

October 11, 2002: Added [Debian](#) vendor statement made 10/08/2002 (DSA-136 posted 07/30/2002)

28 CA-2002-28: Trojan Horse Sendmail Distribution

Original release date: October 08, 2002

Last revised: March 25, 2003

Source: CERT/CC

A complete revision history is at the end of this file.

Overview

The CERT/CC has received confirmation that some copies of the source code for the Sendmail package were modified by an intruder to contain a Trojan horse.

Sites that employ, redistribute, or mirror the Sendmail package should immediately verify the integrity of their distribution.

I. Description

The CERT/CC has received confirmation that some copies of the source code for the Sendmail package have been modified by an intruder to contain a Trojan horse.

The following files were modified to include the malicious code:

```
sendmail.8.12.6.tar.Z  
sendmail.8.12.6.tar.gz
```

These files began to appear in downloads from the FTP server ftp.sendmail.org on or around September 28, 2002. The Sendmail development team disabled the compromised FTP server on October 6, 2002 at approximately 22:15 PDT. It does not appear that copies downloaded via HTTP contained the Trojan horse; however, the CERT/CC encourages users who may have downloaded the source code via HTTP during this time period to take the steps outlined in the [Solution](#) section as a precautionary measure.

The Trojan horse versions of Sendmail contain malicious code that is run during the process of building the software. This code forks a process that connects to a fixed remote server on 6667/tcp. This forked process allows the intruder to open a shell running in the context of the user who built the Sendmail software. There is no evidence that the process is persistent after a reboot of the compromised system. However, a subsequent build of the Trojan horse Sendmail package will re-establish the backdoor process.

II. Impact

An intruder operating from the remote address specified in the malicious code can gain unauthorized remote access to any host that compiled a version of Sendmail from this Trojan horse version of the source code. The level of access would be that of the user who compiled the source code.

It is important to understand that the compromise is to the system that is used to build the Sendmail software and **not** to the systems that run the Sendmail daemon. Because the compromised system creates a tunnel to the intruder-controlled system, the intruder may have a path through network access controls.

III. Solution

Obtain an authentic version of Sendmail

The primary distribution site for Sendmail is

<http://www.sendmail.org/>

Sites that mirror the Sendmail source code are encouraged to verify the integrity of their sources.

Verify software authenticity

We strongly encourage sites that recently downloaded a copy of the Sendmail distribution to verify the authenticity of their distribution, regardless of where it was obtained. Furthermore, we encourage users to inspect any and all software that may have been downloaded from the compromised site. Note that it is not sufficient to rely on the timestamps or sizes of the file when trying to determine whether or not you have a copy of the Trojan horse version.

Verify PGP signatures

The Sendmail source distribution is cryptographically signed with the following PGP key:

```
pub 1024R/678C0A03 2001-12-18 Sendmail Signing Key/2002 <send-  
mail@Sendmail.ORG>  
Key fingerprint = 7B 02 F4 AA FC C0 22 DA 47 3E 2A 9A 9B 35 22 45
```

The Trojan horse copy did not include an updated PGP signature, so attempts to verify its integrity would have failed. The sendmail.org staff has verified that the Trojan horse copies did indeed fail PGP signature checks.

Verify MD5 checksums

In the absence of PGP, you can use the following MD5 checksums to verify the integrity of your Sendmail source code distribution:

Correct versions:

```
73e18ea78b2386b774963c8472cbd309 sendmail.8.12.6.tar.gz  
cebe3fa43731b315908f44889d9d2137 sendmail.8.12.6.tar.Z  
8b9c78122044f4e4744fc447eeafef34 sendmail.8.12.6.tar.sig
```

As a matter of good security practice, the CERT/CC encourages users to verify, whenever possible, the integrity of downloaded software. For more information, see

http://www.cert.org/incident_notes/IN-2001-06.html

Employ egress filtering

Egress filtering manages the flow of traffic as it leaves a network under your administrative control.

In the case of the Trojan horse Sendmail distribution, employing egress filtering can help prevent systems on your network from connecting to the remote intruder-controlled system. Blocking outbound TCP connections to port 6667 from your network reduces the risk of internal compromised machines communicating with the remote system.

Build software as an unprivileged user

Sites are encouraged to build software from source code as an unprivileged, non-root user on the system. This can lessen the immediate impact of Trojan horse software. Compiling software that contains Trojan horses as the root user results in a compromise that is much more difficult to reliably recover from than if the Trojan horse is executed as a normal, unprivileged user on the system.

Recovering from a system compromise

If you believe a system under your administrative control has been compromised, please follow the steps outlined in

[Steps for Recovering from a UNIX or NT System Compromise](#)

Reporting

The CERT/CC is interested in receiving reports of this activity. If machines under your administrative control are compromised, please send mail to cert@cert.org with the following text included in the subject line: "[CERT#33376]".

Appendix A Vendor Information

This appendix contains information provided by vendors for this advisory. As vendors report new information to the CERT/CC, we will update this section and note the changes in our revision history. If a particular vendor is not listed below, we have not received their comments.

Apple Computer, Inc.

Mac OS X and Mac OS X Server do not contain the vulnerability described in this report.

Debian

We can confirm that Debian does **not** ship the version with the trojan horse. Our version pre-dates it.

Red Hat Inc.

"Red Hat Linux has not distributed version 8.12.6 of sendmail and is therefore not affected by this vulnerability"

Xerox

A response to this advisory is available from our web site:

<http://www.xerox.com/security>.

The CERT Coordination Center thanks the staff at the Sendmail Consortium for bringing this issue to our attention.

Feedback can be directed to the authors: Chad Dougherty, Marty Lindner.

Copyright 2002 Carnegie Mellon University

Revision History

October 08, 2002: Initial release
October 09, 2002: Fix simple error in sendmail.org URL
October 09, 2002: Added Red Hat vendor statement
October 09, 2002: Added Debian vendor statement
October 14, 2002: Added Apple Vendor statement
March 25, 2003: Added vendor statement from Xerox

29 CA-2002-29: Buffer Overflow in Kerberos Administration Daemon

Original issue date: October 25, 2002

Last revised: February 25, 2003

Source: CERT/CC

A complete revision history is at the end of this file.

Systems Affected

- MIT Kerberos version 4 and version 5 up to and including krb5-1.2.6
- KTH eBones prior to version 1.2.1 and KTH Heimdal prior to version 0.5.1
- Other Kerberos implementations derived from vulnerable MIT or KTH code

Overview

Multiple Kerberos distributions contain a remotely exploitable buffer overflow in the Kerberos administration daemon. A remote attacker could exploit this vulnerability to gain root privileges on a vulnerable system.

The CERT/CC has received reports that indicate that this vulnerability is being exploited. In addition, MIT advisory [MITKRB5-SA-2002-002](#) notes that an exploit is circulating.

We strongly encourage sites that use vulnerable Kerberos distributions to verify the integrity of their systems and apply patches or upgrade as appropriate.

I. Description

Kerberos is a widely used network protocol that uses strong cryptography to authenticate clients and servers. The Kerberos administration daemon (typically called `kadmind`) handles password change and other requests to modify the Kerberos database. The daemon runs on the master Key Distribution Center (KDC) server of a Kerberos realm.

The code that provides legacy support for the Kerberos 4 administration protocol contains a remotely exploitable buffer overflow. The vulnerable code does not adequately validate data read from a network request. This data is subsequently used as an argument to a `memcpy()` call, which can overflow a buffer allocated on the stack. An attacker does not have to authenticate in order to exploit this vulnerability, and the Kerberos administration daemon runs with root privileges.

Both Massachusetts Institute of Technology ([MIT](#)) and Kungl Tekniska Högskolan ([KTH](#)) Kerberos are affected, as well as operating systems, applications, and other Kerberos implementations that use vulnerable code derived from either the MIT or KTH distributions. In MIT Kerberos 5,

the Kerberos 4 administration daemon is implemented in `kadmind4`. In KTH Kerberos 4 ([eBones](#)), the Kerberos administration daemon is implemented in `kadmind`. KTH Kerberos 5 ([Heimdal](#)) also implements the daemon in `kadmind`; however, the Heimdal daemon is only affected if compiled with Kerberos 4 support. Since the vulnerable Kerberos administration daemon is included in the MIT Kerberos 5 and KTH Heimdal distributions, both Kerberos 4 sites and Kerberos 5 sites that enable support for the Kerberos 4 administration protocol are affected.

Further information about this vulnerability may be found in [VU#875073](#).

MIT has released an advisory that contains information about this vulnerability

<http://web.mit.edu/kerberos/www/advisories/MITKRB5-SA-2002-002-kadm4.txt>

and a document that describes the signature of an attack against `kadmind4`:

http://web.mit.edu/kerberos/www/advisories/2002-002-kadm4_attacksig.txt

The KTH eBones and Heimdal web sites also contain information about this vulnerability:

KTH eBones

<http://www.pdc.kth.se/kth-krb/>

KTH Heimdal

<http://www.pdc.kth.se/heimdal/>

In addition to resolving the vulnerability described in [VU#875073](#), version 0.5.1 of KTH Heimdal contains other fixes related to the KDC and administration servers. See the ChangeLog for more information:

<ftp://ftp.pdc.kth.se/pub/heimdal/src/heimdal-0.5-0.5.1.diff.gz>

This vulnerability has been assigned [CAN-2002-1235](#) by the Common Vulnerabilities and Exposures (CVE) group.

II. Impact

An unauthenticated, remote attacker could execute arbitrary code with root privileges. If an attacker is able to gain control of a master KDC, the integrity of the entire Kerberos realm is compromised, including user and host identities and other systems that accept Kerberos authentication.

III. Solution

Apply a patch or upgrade

Apply the appropriate patch or upgrade as specified by your vendor. See [Appendix A](#) below and the Systems Affected section of [VU#875073](#) for specific information.

Disable vulnerable service

Disable support for the Kerberos 4 administration protocol if it is not needed. In MIT Kerberos 5, this can be achieved by disabling `kadmind4`. For information about disabling all Kerberos 4 support in MIT Kerberos 5 at compile time, see

<http://web.mit.edu/kerberos/www/krb5-1.2/krb5-1.2.6/doc/install.html#SEC24>

In KTH Heimdal, it is necessary to recompile `kadmind` in order to disable support for the Kerberos 4 administration protocol. For information about disabling all Kerberos 4 support in KTH Heimdal at compile time, see

<http://www.pdc.kth.se/heimdal/heimdal.html#Building%20and%20Installing>

This solution will prevent Kerberos 4 administrative clients from accessing the Kerberos database. It will also prevent users with Kerberos 4 clients from changing their passwords. In general, the CERT/CC recommends disabling any service that is not explicitly required.

Block or restrict access

Block access to the Kerberos administration service from untrusted networks such as the Internet. Furthermore, only allow access to the service from trusted administrative hosts. By default, the Kerberos 4 administration daemon listens on `751/tcp` and `751/udp`, and the Kerberos 5 administration daemon listens on `749/tcp` and `749/udp`. It may be necessary to block access to the Kerberos 5 administration service if the daemon also supports the Kerberos 4 administration protocol. This workaround will prevent administrative connections and password change requests from blocked networks. Note that this workaround will not prevent exploitation, but it will limit the possible sources of attacks.

Appendix A Vendor Information

This appendix contains information provided by vendors. When vendors report new information, this section is updated and the changes are noted in the revision history. If a vendor is not listed below, we have not received their comments.

Apple Computer, Inc.

The Kerberos Administration Daemon was included in Mac OS X 10.0, but removed in Mac OS X 10.1 and later.

We encourage sites that use vulnerable Kerberos distributions to verify the integrity of their systems and apply patches or upgrade as appropriate.

Conectiva

Our MIT Kerberos 5 packages in Conectiva Linux 8 do contain the vulnerable `kadmind4` daemon, but it is not used by default nor is it installed as a service.

Updated packages are being uploaded to our ftp server and should be available in a few hours at:

<ftp://atualizacoes.conectiva.com.br/8/>

The krb5-server-1.2.3-3U8_3cl.i386.rpm package contains a patched kadmind4 daemon. An announcement will be sent to our security mailing list a few hours after the upload is complete.

[[CLSA-2002:534 \(English\)](#)]

Cray

Cray, Inc. is not vulnerable as the Kerberos administration daemon is not included in any of our operating systems.

Debian

Please see the Debian [vendor record](#) in VU#875073.

FreeBSD

Both the FreeBSD base Kerberos 4 (kadmind) and Kerberos 5 (k5admind v4 compatibility) daemons were vulnerable and have been corrected as of 23 October 2002. In addition, the heimdal and krb5 ports contained the same vulnerability and have been corrected as of 24 October 2002. A Security Advisory is in progress. [[FreeBSD-SA-02:40.kadmind](#)]

Hewlett-Packard

Source: Hewlett-Packard Company Software Security Response Team

RE: CERT VU#875073 CA-2002-29

cross reference id: SSRT2396

HP's implementation for the following Operating Systems Software are not affected by this potential buffer overflow vulnerability in the kadmind4 daemon.

HP-UX

HP-MPE/ix

HP Tru64 UNIX

HP OpenVMS

HP NonStop Servers

To report potential security vulnerabilities in HP software, send an E-mail message to: security-alert@hp.com

IBM

The IBM pSeries Parallel Systems Support Programs (PSSP) implementation of Kerberos V4 (shipped with PSSP) is potentially vulnerable to the Kerberos V4 administration daemon buffer overflow described in CA-2002-29. For more information, see:

<http://techsupport.services.ibm.com/server/nav?fetch=/spflashes/home.html>

Click on the Service Flash for "Potential Kerberos V4 security vulnerability." This link also contains APAR numbers and solution information.

The IBM Network Authentication Service (NAS) product is not vulnerable to the buffer overflow vulnerability in the kadmind4 daemon. NAS is currently at release 1.3 and is available from the AIX Expansion Pack. The kadmind4 daemon is not part of the NAS product.

KTH Kerberos

The eBones and Heimdal web sites have information about this vulnerability:

KTH eBones

<http://www.pdc.kth.se/kth-krb/>

KTH Heimdal

<http://www.pdc.kth.se/heimdal/>

<ftp://ftp.pdc.kth.se/pub/heimdal/src/heimdal-0.4e.kadmind-patch>

Microsoft Corporation

Microsoft's implementation of Kerberos is not affected by this vulnerability.

MIT Kerberos

MIT has released MIT krb5 Security Advisory 2002-002 that includes a patch and a description of an attack signature:

<http://web.mit.edu/kerberos/www/advisories/MITKRB5-SA-2002-002-kadm4.txt>

http://web.mit.edu/kerberos/www/advisories/2002-002-kadm4_patch.txt

http://web.mit.edu/kerberos/www/advisories/2002-002-kadm4_attacksig.txt

NetBSD

NetBSD has released NetBSD-SA2002-026:

<ftp://ftp.NetBSD.org/pub/NetBSD/security/advisories/NetBSD-SA2002-026.txt.asc>

OpenBSD

OpenBSD has released Security Fix 016 for OpenBSD 3.1 and Security Fix 033 for OpenBSD 3.0.

OpenBSD 3.1

<http://www.openbsd.org/errata31.html#kadmin>

OpenBSD 3.0

<http://www.openbsd.org/errata30.html#kadmin>

Openwall

Openwall GNU/*/Linux is not vulnerable. We don't provide Kerberos.

Red Hat, Inc.

Releases of Red Hat Linux version 6.2 and higher include versions of MIT Kerberos that are vulnerable to this issue; however the vulnerable administration server, kadmind4, has never been enabled by default. We are currently working on producing errata packages. When complete these will be available along with our advisory at the URL below. At the same time users of the Red Hat Network will be able to update their systems using the 'up2date' tool.

<http://rhn.redhat.com/errata/RHSA-2002-242.html>

Sun

The Sun Enterprise Authentication Mechanism (SEAM), Sun's implementation of the Kerberos v5 protocols, is not affected by this issue. SEAM does not include support for the Kerberos v4 protocols and kadmind4 does not exist. Additional information regarding SEAM is available from:

<http://www.sun.com/software/security/kerberos/>

SuSE

SuSE Linux 7.2 and later are shipped with Heimdal Kerberos included, but Kerberos 4 support is disabled in all releases. Therefore, SuSE Linux and SuSE Enterprise Linux are not affected by this bug.

Wind River Systems (BSDI)

No version of BSD/OS is vulnerable to this problem.

Xerox

A response to this advisory is available from our web site:

<http://www.xerox.com/security>.

Appendix B References

- <http://web.mit.edu/kerberos/www/>
- <http://web.mit.edu/kerberos/www/advisories/MITKRB5-SA-2002-002-kadm4.txt>
- http://web.mit.edu/kerberos/www/advisories/2002-002-kadm4_patch.txt
- http://web.mit.edu/kerberos/www/advisories/2002-002-kadm4_attacksig.txt
- <http://web.mit.edu/kerberos/www/krb5-1.2/krb5-1.2.6/doc/install.html#SEC24>
- <http://www.pdc.kth.se/kth-krb/>
- <http://www.pdc.kth.se/heimdal/>
- <http://www.pdc.kth.se/heimdal/heimdal.html#Building%20and%20Installing>
- <ftp://ftp.pdc.kth.se/pub/heimdal/src/heimdal-0.4e.kadmind-patch>

The CERT Coordination Center thanks the MIT and KTH Kerberos development teams for information used in this document.

Authors: Art Manion and Jason A. Rafail

Copyright 2002 Carnegie Mellon University

Revision History

October 25, 2002: Initial release

October 25, 2002: Removed incorrect references to Debian advisory DSA-178 and SuSE advisory SuSE-SA:2002:034, added link to Heimdal 0.4e patch, added link to Debian vendor record in VU#875073

October 26, 2002: Added IBM and Red Hat vendor statements

October 28, 2002: Added link to MIT attack signature, updated MIT vendor statement, added statement thanking MIT and KTH

October 29, 2002: Added Sun vendor statement, corrected kth-krb links

October 30, 2002: Updated IBM vendor statement

November 6, 2002: Updated Conectiva statement

November 15, 2002: Added HP and Cray statements, updated FreeBSD statement, changed wording about other Heimdal 0.5.1 fixes

February 13, 2003: Added Xerox statement

February 25, 2003: Updated Xerox statement

30 CA-2002-30: Trojan Horse tcpdump and libpcap Distributions

Original issue date: November 13, 2002

Last revised: --

Source: CERT/CC

A complete revision history is at the end of this file.

Overview

The CERT/CC has received reports that several of the released source code distributions of the libpcap and tcpdump packages were modified by an intruder and contain a Trojan horse.

We strongly encourage sites that use, redistribute, or mirror the libpcap or tcpdump packages to immediately verify the integrity of their distribution.

I. Description

The CERT/CC has received reports that some copies of the source code for libpcap, a packet acquisition library, and tcpdump, a network sniffer, have been modified by an intruder and contain a Trojan horse.

The following distributions were modified to include the malicious code:

tcpdump

md5sum 3a1c2dd3471486f9c7df87029bf2f1e9 tcpdump-3.6.2.tar.gz

md5sum 3c410d8434e63fb3931fe77328e4dd88 tcpdump-3.7.1.tar.gz

libpcap

md5sum 73ba7af963aff7c9e23fa1308a793dca libpcap-0.7.1.tar.gz

These modified distributions began to appear in downloads from the HTTP server www.tcpdump.org on or around Nov 11 2002 10:14:00 GMT. The tcpdump development team disabled download of the distributions containing the Trojan horse on Nov 13 2002 15:05:19 GMT. However, the availability of these distributions from mirror sites is unknown. At this time, it does not appear that related projects such as WinPcap and WinDump contain this Trojan horse.

The Trojan horse version of the tcpdump source code distribution contains malicious code that is run when the software is compiled. This code, executed from the tcpdump `configure` script, will attempt to connect (via `wget`, `lynx`, or `fetch`) to port 80/tcp on a fixed hostname in order to download a shell script named `services`. In turn, this downloaded shell script is executed to generate a C file (`conftes.c`), which is subsequently compiled and run.

When executed, `confetes.c` makes an outbound connection to a fixed IP address (corresponding to the fixed hostname used in the `configure` script) on port 1963/tcp and reads a single byte. Three possible values for this downloaded byte are checked, each causing `confetes.c` to respond in different ways:

- 'A' will cause the Trojan horse to exit
- 'D' will cause the Trojan to fork itself, spawn a shell, and redirect this shell to the connected IP address (Note that communication to and from this shell is obfuscated by XORing all bytes with the constant 0x89.)
- 'M' will cause the Trojan horse to close the connection and sleep for 3600 seconds

To mask the activity of this Trojan horse in tcpdump, libpcap, the underlying packet-capture library of tcpdump, has been modified (`gencode.c`) to explicitly ignore all traffic on port 1963 (i.e., a BPF expression of `"not port 1963"`).

II. Impact

An intruder operating from (or able to impersonate) the remote address specified in the malicious code could gain unauthorized remote access to any host that compiled a version of tcpdump with this Trojan horse. The privilege level under which this malicious code would be executed would be that of the user who compiled the source code.

III. Solution

We encourage sites using libpcap and tcpdump to verify the authenticity of their distribution, regardless of where it was obtained.

Where to get libpcap and tcpdump

While the compromise of these distributions is being investigated, the tcpdump and libpcap maintainers recommend using the following distribution sites:

<http://sourceforge.net/projects/tcpdump/>

<http://sourceforge.net/projects/libpcap/>

Sites that mirror the source code are encouraged to verify the integrity of their sources. We also encourage users to inspect any and all other software that may have been downloaded from the compromised site. Note that it is not sufficient to rely on the timestamps or sizes of the file when trying to determine whether or not you have a copy of the Trojan horse version.

Verifying checksums

The MD5 hashes of the vendor suggested updates for libpcap and tcpdump are as follows:

tcpdump

```
md5sum 03e5eac68c65b7e6ce8da03b0b0b225e tcpdump-3.7.1.tar.gz
```

libpcap

md5sum 0597c23e3496a5c108097b2a0f1bd0c7 libpcap-0.7.1.tar.gz

As a matter of good security practice, the CERT/CC encourages users to verify, whenever possible, the integrity of downloaded software. For more information, see

http://www.cert.org/incident_notes/IN-2001-06.html

Appendix A Vendor Information

This appendix contains information provided by vendors for this advisory. As vendors report new information to the CERT/CC, we will update this section and note the changes in our revision history. If a particular vendor is not listed below, we have not received their comments.

Conectiva

We have checked all our released libpcap and tcpdump packages and confirmed that they do not contain the trojan code.

Debian

Problematic packages are only distributed in Debian/unstable. I have examined both source packages and they did not contain the trojan code the HLUg reported on their web page. Hence, I guess that Debian distributes safe source.

MontaVista Software, Inc.

We have examined our sources, and our software does not contain this trojan. We are not vulnerable to this advisory.

SuSE

SuSE Linux products are not vulnerable.

Feedback can be directed to the authors: Roman Danyliw, Chad Dougherty.

Copyright 2002 Carnegie Mellon University

Revision History

November 13, 2002: Initial release

31 CA-2002-31: Multiple Vulnerabilities in BIND

Original release date: November 14, 2002

Last revised: Tue Apr 29 17:46:04 EST 2003

Source: CERT/CC

A complete revision history can be found at the end of this file.

Systems Affected

- Systems running various versions of BIND 4 and BIND 8

Because the normal operation of most services on the Internet depends on the proper operation of DNS servers, other services could be affected if these vulnerabilities are exploited.

Overview

Multiple vulnerabilities with varying impacts have been found in BIND, the popular domain name server and client library software package from the Internet Software Consortium (ISC).

Some of these vulnerabilities may allow remote attackers to execute arbitrary code with the privileges of the user running *named*, (typically root), or with the privileges of vulnerable client applications. The other vulnerabilities will allow remote attackers to disrupt the normal operation of DNS name service running on victim servers.

I. Description

Multiple vulnerabilities have been found in BIND (Berkeley Internet Name Domain). One of these vulnerabilities (VU#852283) may allow remote attackers to execute arbitrary code with the privileges of the user running *named*, typically root. Other vulnerabilities (VU#229595, VU#581682) may allow remote attackers to disrupt the normal operation of your name server, possibly causing a crash. A vulnerability in the DNS resolver library (VU#844360) may allow remote attackers to execute arbitrary code with the privileges of applications that issue network name or address requests.

BIND DNS Server Vulnerabilities

VU#852283 - *Cached malformed SIG record buffer overflow*

This vulnerability is a buffer overflow in *named*. It can occur when responses are constructed using previously-cached malformed SIG records. (SIG records are typically associated with cryptographically signed DNS data.) Exploitation of the vulnerability can lead to arbitrary code execution as the *named* uid, typically root.

The following versions of BIND are affected:

- BIND versions 4.9.5 to 4.9.10
- BIND versions 8.1, 8.2 to 8.2.6, and 8.3.0 to 8.3.3

VU#229595 - *Overly large OPT record assertion*

ISC BIND 8 fails to properly handle DNS lookups for non-existent sub-domains when overly large OPT resource records are appended to a query. When a non-existent domain (NXDOMAIN) response is constructed by a victim nameserver, an assertion may be triggered if the client passes a large UDP buffer size. This assertion will cause the running *named* to exit.

The following versions of BIND are affected:

- BIND versions 8.3.0 to 8.3.3

VU#581682 - *ISC BIND 8 fails to properly de-reference cache SIG RR elements with invalid expiry times from the internal database*

ISC's description of this vulnerability states:

It is possible to de-reference a NULL pointer for certain signature expire values.

The following versions of BIND are affected:

- BIND versions 8.2 to 8.2.6
- BIND versions 8.3.0 to 8.3.3.

BIND DNS Resolver Vulnerabilities

VU#844360 - *Domain Name System (DNS) stub resolver libraries vulnerable to buffer overflows via network name or address lookups*

The stub resolver library in BIND 4 contains buffer overflows in code that handles responses for network name and address requests. Note that these overflows are distinct from the issues discussed in CA-2002-19 and VU#738331.

The following DNS stub resolver libraries are known to be affected:

- BIND 4.9.2 through 4.9.10

The status of other resolver libraries derived from BIND 4 such as BSD libc, GNU glibc, and those used by System V UNIX systems is currently unknown. These issues map to CVE as follows:

VU#852283 - CAN-2002-1219

VU#229595 - CAN-2002-1220

VU#581682 - CAN-2002-1221

VU#844360 - CAN-2002-0029

II. Impact

VU#852283 - *Cached malformed SIG record buffer overflow*

A remote attacker could execute arbitrary code on the nameserver with the privileges of the *named* uid, typically root.

VU#229595 - *Overly large OPT record assertion*

A remote attacker can disrupt the normal operation of your name server, possibly causing a crash.

VU#581682 - *ISC BIND 8 fails to properly de-reference cache SIG RR elements with invalid expiry times from the internal database*

A remote attacker can disrupt the normal operation of your name server, possibly causing a crash.

VU#844360 - *Domain Name System (DNS) stub resolver libraries vulnerable to buffer overflows via network name or address lookups*

A remote attacker could execute arbitrary code with the privileges of the application that made the request or cause a denial of service. The attacker would need to control DNS responses possibly by spoofing the responses or by gaining sufficient access to a DNS server.

III. Solution

Apply a patch from your vendor.

Appendix A contains information provided by vendors for this advisory. As vendors report new information to the CERT/CC, we will update this section and note the changes in our revision history. If a particular vendor is not listed below, we have not received their comments. Please contact your vendor directly.

If a vendor patch is not available, you may wish to consider applying the patches ISC has produced:

BIND 8.3.3 - <http://www.isc.org/products/BIND/patches/bind833.diff>

BIND 8.2.6 - <http://www.isc.org/products/BIND/patches/bind826.diff>

BIND 4.9.10 - <http://www.isc.org/products/BIND/patches/bind4910.diff>

For VU#844360, the BIND 4 *libresolv* buffer overflows, an upgrade to a corrected version of the DNS resolver libraries will be required.

Note that DNS resolver libraries can be used by multiple applications on most systems. It may be necessary to upgrade or apply multiple patches and then recompile statically linked applications.

Applications that are *statically* linked must be recompiled using patched resolver libraries. Applications that are *dynamically* linked do not need to be recompiled; however, running services need to be restarted in order to use the patched resolver libraries.

System administrators should consider the following process when addressing this issue:

1. Patch or obtain updated resolver libraries.
2. Restart any dynamically linked services that use the resolver libraries.
3. Recompile any statically linked applications using the patched or updated resolver libraries.

Workarounds

[VU#852283](#) - *Cached malformed SIG record buffer overflow*

[VU#229595](#) - *Overly large OPT record assertion*

[VU#581682](#) - *ISC BIND 8 fails to properly dereference cache SIG RR elements with invalid expiry times from the internal database*

One potential workaround to limit exposure to the vulnerabilities in *named* is to disable recursion on any nameserver responding to DNS requests made by untrusted systems. As mentioned in [Securing an Internet Name Server](#):

Disabling recursion puts your name servers into a passive mode, telling them never to send queries on behalf of other name servers or resolvers. A totally non-recursive name server is protected from cache poisoning, since it will only answer queries directed to it. It doesn't send queries, and hence doesn't cache any data. Disabling recursion can also prevent attackers from bouncing denial of services attacks off your name server by querying for external zones.

Non-recursive nameservers should be much more resistant to exploitation of the server vulnerabilities listed above.

Additional Countermeasures

ISC recommends upgrading to BIND version 9.2.1. BIND version 9.2.1 is available from: <http://www.isc.org/products/BIND/bind9.html>.

Note that the upgrade from previous versions of BIND may require additional site reconfiguration.

Appendix A Vendor Information

This appendix contains information provided by vendors for this advisory. As vendors report new information to the CERT/CC, we will update this section and note the changes in our revision history. If a particular vendor is not listed below, we have not received their comments.

Alcatel

Following CERT advisory CA-2002-31 on security vulnerabilities in the ISC BIND implementation, Alcatel has conducted an immediate assessment to determine any impact this may have on our portfolio. A first analysis has shown that the following products (OmniSwitch 6600, 7700, 8800) may be impacted. Customers may wish to contact their support for more details. The security of our customers' networks is of highest priority for Alcatel. Therefore we continue to test our product portfolio against potential ISC BIND security vulnerabilities and will provide updates if necessary.

Apple

Affected Systems: Mac OS X and Mac OS X Server with BIND versions 8.1, 8.2 to 8.2.6, and 8.3.0 to 8.3.3

Mitigating Factors: BIND is not enabled by default on Mac OS X or Mac OS X Server

This is addressed in Security Update 2002-11-21
http://www.apple.com/support/security/security_updates.html

Conectiva

Conectiva Linux 6.0 is affected by this. Updated packages are available at our ftp server: ftp://atualizacoes.conectiva.com.br/6.0/RPMS/bind-8.2.6-1U60_2cl.i386.rpm
ftp://atualizacoes.conectiva.com.br/6.0/RPMS/bind-chroot-8.2.6-1U60_2cl.i386.rpm
ftp://atualizacoes.conectiva.com.br/6.0/RPMS/bind-devel-8.2.6-1U60_2cl.i386.rpm
ftp://atualizacoes.conectiva.com.br/6.0/RPMS/bind-devel-static-8.2.6-1U60_2cl.i386.rpm
ftp://atualizacoes.conectiva.com.br/6.0/RPMS/bind-doc-8.2.6-1U60_2cl.i386.rpm
ftp://atualizacoes.conectiva.com.br/6.0/RPMS/bind-utils-8.2.6-1U60_2cl.i386.rpm

An advisory about this vulnerability is pending and should be sent to our security mailing list and published in our web site during the day (Nov 14th).

Cray Inc.

Cray Inc. may be vulnerable and has opened spr 723892 to investigate.

Debian GNU/Linux

Debian (among other GNU/Linux distributors) was very unhappy to learn that ISC knew about this vulnerability since mid October and that the advisory was released without patches, so only

paying members of the ISC forum were able to provide updates to their customers. However, after the patches were finally released to the public, Debian was able to provide fixed packages as well. They are announced in DSA 196 .

FreeBSD

Please see FreeBSD-SA-02:43.bind.

GNU glibc

Version 2.3.1 of the GNU C Library is vulnerable. Earlier versions are also vulnerable. The following patch has been installed into the CVS sources, and should appear in the next version of the GNU C Library. This patch is also available from the following URL:

http://sources.redhat.com/cgi-bin/cvsweb.cgi/libc/resolv/nss_dns/dns-network.c.diff?r1=1.17&r2=1.15&cvsroot=glibc

2002-11-18 Roland McGrath

```
* resolv/nss_dns/dns-network.c (getanswer_r): In BYNAME case, search
all aliases for one that matches the ".IN-ADDR.ARPA" form.
Do the parsing inline instead of copying strings and calling
inet_network, and properly skip all alias names not matching the
form.
```

2002-11-14 Paul Eggert

```
* resolv/nss_dns/dns-network.c (getanswer_r): Check for buffer
overflow when skipping the question part and when unpacking aliases.
```

```
=====
```

```
RCS file: /cvs/glibc/libc/resolv/nss_dns/dns-network.c,v
```

```
retrieving revision 1.15
```

```
retrieving revision 1.17
```

```
diff -u -r1.15 -r1.17
```

```
--- libc/resolv/nss_dns/dns-network.c 2002/10/17 21:49:12 1.15
```

```
+++ libc/resolv/nss_dns/dns-network.c 2002/11/19 06:40:16 1.17
```

```
@@ -283,7 +283,15 @@
```

```
/* Skip the question part. */
while (question_count-- > 0)
- cp += __dn_skipname (cp, end_of_message) + QFIXEDSZ;
+ {
+ int n = __dn_skipname (cp, end_of_message);
+ if (n < 0 || end_of_message - (cp + n) < QFIXEDSZ)
+ {
+ __set_h_errno (NO_RECOVERY);
+ return NSS_STATUS_UNAVAIL;
+ }
+ cp += n + QFIXEDSZ;
```

```

+ }
  alias_pointer = result->n_aliases = &net_data->aliases[0];
  *alias_pointer = NULL;
@@ -344,64 +352,94 @@
  return NSS_STATUS_UNAVAIL;
  }
  cp += n;
-     *alias_pointer++ = bp;
-     n = strlen (bp) + 1;
-     bp += n;
-     linebuflen -= n;
-     result->n_addrtype = class == C_IN ? AF_INET : AF_UNSPEC;
-     ++have_answer;
+ if (alias_pointer + 2 < &net_data->aliases[MAX_NR_ALIASES])
+ {
+ *alias_pointer++ = bp;
+ n = strlen (bp) + 1;
+ bp += n;
+ linebuflen -= n;
+ result->n_addrtype = class == C_IN ? AF_INET : AF_UNSPEC;
+ ++have_answer;
+ }
  }
  }
  if (have_answer)
  {
- char *tmp;
- int len;
- char *in, *cp, *rp, *wp;
- int cnt, first_flag;
-
  *alias_pointer = NULL;
  switch (net_i)
  {
case BYADDR:
-     result->n_name = result->n_aliases[0];
+     result->n_name = *result->n_aliases++;
  result->n_net = 0L;
-     break;
-     case BYNAME:
-     len = strlen (result->n_aliases[0]);
-     tmp = (char *) alloca (len + 1);
-     tmp[len] = 0;
-     wp = &tmp[len - 1];

```

```

-
-     rp = in = result->n_aliases[0];
-     result->n_name = ans;
-
-     first_flag = 1;
-     for (cnt = 0; cnt < 4; ++cnt)
-     {
-     char *startp;
+     return NSS_STATUS_SUCCESS;
-     startp = rp;
-     while (*rp != '.')
-         ++rp;
-     if (rp - startp > 1 || *startp != '0' || !first_flag)
-     {
-         first_flag = 0;
-         if (cnt > 0)
-             *wp-- = '.';
-         cp = rp;
-         while (cp > startp)
-             *wp-- = *--cp;
-     }
-     in = rp + 1;
-     }
-
-     result->n_net = inet_network (wp);
+ case BYNAME:
+     {
+     char **ap = result->n_aliases++;
+     while (*ap != NULL)
+     {
+         /* Check each alias name for being of the forms:
+         4.3.2.1.in-addr.arpa      = net 1.2.3.4
+         3.2.1.in-addr.arpa       = net 0.1.2.3
+         2.1.in-addr.arpa         = net 0.0.1.2
+         1.in-addr.arpa           = net 0.0.0.1
+         */
+         uint32_t val = 0;         /* Accumulator for n_net
value. */
+         unsigned int shift = 0; /* Which part we are parsing
now. */
+         const char *p = *ap; /* Consuming the string. */
+         do
+         {
+             /* Match the leading 0 or 0[xX] base indicator. */

```

```

+         unsigned int base = 10;
+         if (*p == '0' && p[1] != '.')
+         {
+             base = 8;
+             ++p;
+             if (*p == 'x' || *p == 'X')
+             {
+                 base = 16;
+                 ++p;
+                 if (*p == '.')
+                     break; /* No digit here. Give up on alias. */
+             }
+             if (*p == '\\0')
+                 break;
+         }
+
+         uint32_t part = 0; /* Accumulates this part's number. */
+         do
+         {
+             if (isdigit (*p) && (*p - '0' < base))
+                 part = (part * base) + (*p - '0');
+             else if (base == 16 && isxdigit (*p))
+                 part = (part << 4) + 10 + (tolower (*p) - 'a');
+             ++p;
+         } while (*p != '\\0' && *p != '.');
+
+         if (*p != '.')
+             break; /* Bad form. Give up on this name. */
+
+         /* Install this as the next more significant byte. */
+         val |= part << shift;
+         shift += 8;
+         ++p;
+
+         /* If we are out of digits now, there are two cases:
+         1. We are done with digits and now see "in-addr.arpa".
+         2. This is not the droid we are looking for. */
+         if (!isdigit (*p) && !strcasecmp (p, "in-addr.arpa"))
+         {
+             result->n_net = val;

```

```

+             return NSS_STATUS_SUCCESS;
+         }
+
+         /* Keep going when we have seen fewer than 4 parts.
+ */
+         } while (shift < 32);
+     }
+ }
break;
}
-
- ++result->n_aliases;
- return NSS_STATUS_SUCCESS;
}
__set_h_errno (TRY_AGAIN);

```

Hewlett-Packard Company

SOURCE: Hewlett-Packard Company Software Security Response team x-ref: SSRT2408

At the time of writing this document, Hewlett Packard is currently investigating the potential impact to HP's released Operating System software products. As further information becomes available HP will provide notice of the availability of any necessary patches through standard security bulletin announcements and be available from your normal HP Services support channel.

IBM Corporation

The AIX operating system is vulnerable to the named and DNS resolver issues in releases 4.3.3, 5.1.0 and 5.2.0. The following APARs are available:

AIX 4.3.3 APAR IY37088 (available)

AIX 5.1.0 APAR IY37091 (available)

AIX 5.2.0 APAR IY37289 (available)

MandrakeSoft

Linux-Mandrake 7.2 and Single Network Firewall 7.2 are the only supported distributions to ship with BIND8; all other supported distributions ship with BIND9 and are thus not vulnerable. Updates for Linux-Mandrake 7.2 and Single Network Firewall 7.2 will be made available shortly. These updates will consist of BIND9 packages and patched BIND8 packages, although MandrakeSoft recommends that everyone able to, upgrade to the BIND9 packages.

MetaSolv

MetaSolv Statement ref:CERTR Advisory CA-2002-31

The BIND code embedded in the DNS Server (Based on ISC BIND 8.2.3) on both MetaSolv Policy Services 4.1 and 4.2 (base) are partially vulnerable to CERTR Advisory CA-2002-31. This issue is being tracked by MetaSolv under Case #28231. In particular:

VU#844360 - Domain Name System (DNS) stub resolver libraries vulnerable to buffer overflows via network name or address lookups (VU#852283 - CAN-2002-1219 / VU#229595 - CAN-2002-1220 / VU#581682 - CAN-2002-1221/ VU#844360 - CAN-2002-0029) was addressed in Policy Services 4.2 Service Pack 1 efix 1. The vulnerability can be avoided by upgrading to Policy Services 4.2 Service Pack 1 efix 1 from MetaSolv Policy Services 4.1 and 4.2 (base). The efix includes all ISC sanctioned patches to BIND 8.2.6. to remedy this vulnerability. Please contact MetaSolv Global Customer Care (supporthd@metasolv.com) for assistance.

VU#229595 - Overly large OPT record assertion on BIND 8.3.x does not affect the current distribution as the base is on ISC BIND 8.2.6 and the ISC Sanctioned Patches to 8.2.6 in 4.2 Service Pack 1 efix 1. No action is required in Policy Services 4.1 and 4.2 (base) or Policy Services 4.2 Service Pack 1 efix 1 for this vulnerability.

VU#852283 - Cached malformed SIG record buffer overflow and VU#581682 - ISC BIND 8 fails to properly de-reference cache SIG RR elements with invalid expiry times from the internal database. The ISC sanctioned library changes to 8.2.6. have been applied to 4.2 Service Pack 1 and are currently undergoing load and integration testing and will be available as Policy Services 4.2 Service Pack 1 efix 2 on 11/22/02. Please contact MetaSolv Global Customer Care (supporthd@metasolv.com) for availability and assistance.

Microsoft Corporation

Microsoft products do not use the program in question. Microsoft products are not affected by this issue.

MontaVista Software

MontaVista ships BIND 9, thus is not vulnerable to these advisories.

Nominum, Inc.

Nominum "Foundation" Authoritative Name Server (ANS) is not affected by this vulnerability. Also, Nominum "Foundation" Caching Name Server (CNS) is not affected by this vulnerability. Nominum's commercial DNS server products, which are part of Nominum "Foundation" IP Address Suite, are not based on BIND and do not contain any BIND code, and so are not affected by vulnerabilities discovered in any version of BIND.

Nortel Networks

NetID version 4.3.1 and below is affected by the vulnerabilities identified in CERT/CC Advisory CA-2002-31. A bulletin and patched builds are available from the following Nortel Networks support contacts:

North America: 1-800-4NORTEL or 1-800-466-7835

Europe, Middle East and Africa: 00800 8008 9009, or +44 (0) 870 907 9009

Optivity NMS is not affected.

Openwall Project

BIND 4.9.10-OW2 includes the patch provided by ISC and thus has the two vulnerabilities affecting BIND 4 fixed. Previous versions of BIND 4.9.x-OW patches, if used properly, significantly reduced the impact of the "named" vulnerability. The patches are available at their usual location:

<http://www.openwall.com/bind/>

A patch against BIND 4.9.11 will appear as soon as this version is officially released, although it will likely be effectively the same as the currently available 4.9.10-OW2. It hasn't been fully researched whether the resolver code in glibc, and in particular on Openwall GNU/*/Linux, shares any of the newly discovered BIND 4 resolver library vulnerabilities. Analysis is in progress.

Red Hat Inc.

Older releases (6.2, 7.0) of Red Hat Linux shipped with versions of BIND which may be vulnerable to these issues however a Red Hat security advisory in July 2002 upgraded all our supported distributions to BIND 9.2.1 which is not vulnerable to these issues.

All users who have BIND installed should ensure that they are running these updated versions of BIND.

<http://rhn.redhat.com/errata/RHSA-2002-133.html> Red Hat Linux

<http://rhn.redhat.com/errata/RHSA-2002-119.html> Advanced Server 2.1

Sun Microsystems

The Solaris DNS resolver library (libresolv(3LIB)) is affected by VU#844360 in the following supported versions of Solaris:

Solaris 2.6

The Solaris BIND (in.named(1M)) daemon is affected by VU#852283 and VU#581682 in the following supported versions of Solaris:

Solaris 7, 8, and 9

The Solaris BIND (in.named(1M)) daemon is affected by VU#229595 in the following supported versions of Solaris:

Solaris 9

Patches are being generated for all of the above releases. Sun will be publishing a Sun Alert for this issue at the following location shortly:

<http://sunsolve.Sun.COM/pub-cgi/retrieve.pl?doc=fsalert%2F48818>

The patches will be available from:

<http://sunsolve.sun.com/securitypatch>

Xerox

A response to this vulnerability [VU#229595, VU#844360, VU#852283] is available from our web site: <http://www.xerox.com/security>.

Appendix B References

1. "Securing an Internet Name Server" - <http://www.cert.org/archive/pdf/dns.pdf>
2. "Internet Security Systems Security Advisory - Multiple Remote Vulnerabilities in BIND4 and BIND8" - <http://bvlive01.iss.net/issEn/delivery/xforce/alertdetail.jsp?oid=21469>
3. "BIND Vulnerabilities" - <http://www.isc.org/products/BIND/bind-security.html>
4. "RFC2671 - Extension Mechanisms for DNS (EDNS0)" - <ftp://ftp.isi.edu/in-notes/rfc2671.txt>

Internet Security Systems publicly reported the following issues VU#852283, VU#229595, and VU#581682.

We thank ISC for their cooperation.

Authors: [Ian A. Finlay](#), [Jeffrey S. Havrilla](#), [Art Manion](#), and [Jeffrey J. Carpenter](#)

Copyright 2002 Carnegie Mellon University

Revision History

November 14, 2002: Initial release
November 14, 2002: Added vendor statement for MandrakeSoft
November 14, 2002: Added vendor statement for Cray Inc.
November 14, 2002: Re-worded VU#844360 overview, description, and impact, added indentation
November 14, 2002: Added vendor statement for Microsoft Corporation
November 14, 2002: Added vendor statement for Debian GNU/Linux
November 15, 2002: Added vendor statement for IBM
November 15, 2002: Added vendor statement for MetaSolv
November 15, 2002: Added vendor statement for Sun
November 15, 2002: Added vendor statement for Nortel
November 21, 2002: Added vendor statement for Apple

December 03, 2002: Revised vendor statement for Nortel (note their update was sent on Nov 27, 2002)

December 09, 2002: Revised vendor statement for IBM

February 25, 2003: Added vendor statement for Alcatel

February 26, 2003: Added vendor statement for glibc

February 27, 2003: Updated vendor statement for IBM

April 29, 2003: Added vendor statement for Xerox

32 CA-2002-32: Backdoor in Alcatel OmniSwitch AOS

Original release date: November 21, 2002
Last revised: Thu Jan 2 13:02:38 EST 2003
Source: CERT/CC, Alcatel

A complete revision history can be found at the end of this file.

Systems Affected

- Alcatel OmniSwitch 7700/7800 switches running Alcatel Operating System (AOS) version 5.1.1

Overview

Alcatel has recently discovered a serious vulnerability in AOS version 5.1.1. Exploitation of this vulnerability can lead to full administrative control of the device running AOS.

I. Description

AOS typically runs on network infrastructure devices, such as the Alcatel OmniSwitch 7000 series switch. According to Alcatel:

During an NMAP audit of the AOS 5.1.1 code that runs on the Alcatel OmniSwitch 7700/7800 LAN switches, it was determined a telnet server was listening on TCP port number 6778. This was used during development to access the Wind River Vx-Works operating system. Due to an oversight, this access was not removed prior to product release.

Further information about this vulnerability may be found in VU#181721. This issue is also being referenced as CAN-2002-1272:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-1272>

II. Impact

An attacker can gain full access to any device running AOS version 5.1.1, which can result in, but is not limited to, unauthorized access, unauthorized monitoring, information leakage, or denial of service.

III. Solution

Upgrade to AOS 5.1.1.R02 or AOS 5.1.1.R03

Contact Alcatel's customer support for the updated AOS.

Workarounds

Block access to port 6778/TCP at your network perimeter.

Appendix A Vendor Information

VU#181721 was written by Alcatel. As new vendor information is reported to the CERT/CC, we will update VU#181721 and note the changes in our revision history.

Appendix B References

1. VU#181721: Alcatel OmniSwitch 7700/7800 does not require a password for accessing the telnet server - <http://www.kb.cert.org/vuls/id/181721>
2. OmniSwitch_7000_brief - http://www.ind.alcatel.com/nextgen/OmniSwitch_7000_brief.pdf
3. CAN-2002-1272 - <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-1272>

We thank Olivier Paridaens and Jeff Hayes of Alcatel for reporting this issue.

Author: Ian A. Finlay

Copyright 2002 Carnegie Mellon University

Revision History

November 21, 2002: Initial release

January 02, 2002: Changed URL for Alcatel Customer Support

33 CA-2002-33: Heap Overflow Vulnerability in Microsoft Data Access Components (MDAC)

Original release date: November 21, 2002

Last revised: --

Source: CERT/CC

A complete revision history can be found at the end of this file.

Systems Affected

All Microsoft Windows systems running the following:

- Versions of Microsoft Data Access Components (MDAC) prior to 2.7
- Internet Explorer version 6
- Internet Explorer version 5.5
- Internet Explorer version 5.1

Note that Microsoft Windows XP is shipped with MDAC version 2.7 and is not vulnerable by default even though Internet Explorer 6.0 is installed.

Because the normal operation of several applications and web servers on a system depend on the proper operation of the MDAC ActiveX control, other programs could be used as an exploit vector. For example, Internet Information Server may be configured to use MDAC.

Overview

A vulnerability in the Microsoft Data Access Components (MDAC) could lead to remote execution of code with the privileges of the current process or user.

I. Description

Microsoft Data Access Components (MDAC) is a collection of utilities and routines to process requests between databases and network applications. A buffer overflow vulnerability exists in the Remote Data Services (RDS) component of MDAC.

The RDS component provides an intermediary step for a client's request for service from a back-end database that enables the web site to apply business logic to the request.

According to [Microsoft's Security Bulletin MS02-065](#), a routine in the RDS component, specifically the RDS Data Stub function, contains an unchecked buffer. The RDS Data Stub function's purpose is to parse incoming HTTP requests and generate RDS commands. This unchecked buffer could be exploited to cause a heap overflow.

There are two ways in which this vulnerability can be exploited. The first involves an attacker sending a malicious HTTP request to a vulnerable service, such as an IIS server. If RDS is enabled, the attacker can execute arbitrary code as the IIS server. RDS is not enabled by default on Windows 2000 and Windows XP systems. It can be disabled on other systems by following the advice in Microsoft's security bulletin.

The other way to exploit this vulnerability involves a malicious web site hosting a page that exploits the buffer overflow in the MDAC RDS stub through a client application, such as Internet Explorer. Most systems running Internet Explorer on operating systems other than Windows XP are vulnerable to this attack. The attacker is able to run arbitrary code as the user viewing the malicious web page.

Both web servers and client applications that rely on MDAC are affected. It is recommended that all users of Microsoft Windows 98, Windows 98 SE, Windows ME, Windows NT 4.0, and Windows 2000 apply the [patch \(Q329414\)](#). Windows XP users are not affected since MDAC 2.7, the non-vulnerable version, is installed by default.

Information about this vulnerability is discussed in [VU#542081](#). This issue is also being referenced as [CAN-2002-1142](#).

II. Impact

A remote attacker could execute arbitrary code with the privileges of the application that processed the request.

In the case of a web server or other service, this is likely to be the SYSTEM or another account with elevated privileges. In the case of a client application, this will be the account used to view the web page.

III. Solution

Apply a patch from your vendor.

Microsoft has released a [patch \(Q329414\)](#) and a [security bulletin \(MS02-065\)](#) to address this issue. An end-user version of MS02-065 is available at http://www.microsoft.com/security/security_bulletins/ms02-065.asp.

According to the Microsoft advisory, a scenario exists in by which a vulnerable version of the control may be re-installed on a Windows system even after the patch has been applied. This is due to the fact that the vulnerable ActiveX control is signed by Microsoft and the patch does not set the kill bit for the MDAC control.

This vulnerability was reported in an [advisory](#) by Foundstone and in [MS02-065](#) by Microsoft.

Copyright 2002 Carnegie Mellon University

Revision History

November 21, 2002: Initial release

34 CA-2002-34: Buffer Overflow in Solaris X Window Font Service

Original release date: November 25, 2002

Last revised: Tue Dec 17 08:17:32 EST 2002

Source: CERT/CC

A complete revision history can be found at the end of this file.

Systems Affected

- Sun Microsystems Solaris 2.5.1 (Sparc/Intel)
- Sun Microsystems Solaris 2.6 (Sparc/Intel)
- Sun Microsystems Solaris 7 (Sparc/Intel)
- Sun Microsystems Solaris 8 (Sparc/Intel)
- Sun Microsystems Solaris 9 (Sparc)

Overview

The Solaris X Window Font Service (XFS) daemon (fs.auto) contains a remotely exploitable buffer overflow vulnerability that could allow an attacker to execute arbitrary code or cause a denial of service.

I. Description

A remotely exploitable buffer overflow vulnerability exists in the Solaris X Window Font Service (XFS) daemon (fs.auto). Exploitation of this vulnerability can lead to arbitrary code execution on a vulnerable Solaris system. This vulnerability was discovered by ISS X-Force.

The Solaris X Window Font Service (XFS) serves font files to clients. Sun describes the XFS service as follows:

The X Font Server is a simple TCP/IP-based service that serves font files to its clients. Clients connect to the server to request a font set, and the server reads the font files off the disk and serves them to the clients. The X Font Server daemon consists of a server binary /usr/openwin/bin/xf.

The XFS daemon is installed and running by default on all versions of the Solaris operating system. Further information about this vulnerability may be found in VU#312313.

<http://www.kb.cert.org/vuls/id/312313>

This vulnerability is also being referred to as CAN-2002-1317 by CVE.

Note this vulnerability is in the X Window Font Server, and *not* the filesystem of a similar name.

II. Impact

A remote attacker can execute arbitrary code with the privileges of the fs.auto daemon (typically nobody) or cause a denial of service by crashing the service.

III. Solution

Apply a patch from your vendor

Appendix A contains information provided by vendors for this advisory. As vendors report new information to the CERT/CC, we will update this section and note the changes in our revision history. If a particular vendor is not listed below, we have not received their comments. Please contact your vendor directly.

Disable vulnerable service

Until patches can be applied, you may wish to disable the XFS daemon (fs.auto). As a best practice, the CERT/CC recommends disabling all services that are not explicitly required. On a typical Solaris system, it should be possible to disable the fs.auto daemon by commenting out the relevant entries in `/etc/inetd.conf` and then restarting the `inetd` process.

Workarounds

Block access to port 7100/TCP at your network perimeter. Note that this will not protect vulnerable hosts within your network perimeter.

Appendix A Vendor Information

Hewlett-Packard Company

HEWLETT-PACKARD COMPANY
SECURITY BULLETIN: HPSBUX0212-228
Originally issued: 4 Dec 2002

reference id: CERT CA-2002-34, SSRT2429

HP Published Security Bulletin HPSBUX0212-228 with solutions for HP 9000 Series 700 and 800 running HP-UX 10.10, 10.20, 10.24, 11.00, 11.04, 11.11, and 11.22

This bulletin is available from the HP IT Resource Center page at: <http://itrc.hp.com> "Maintenance and Support" then "Support Information Digests" and then "hp security bulletins archive" search for bulletin HPSBUX0212-228.

NOT IMPACTED:

HP Tru64 UNIX, HP NonStop Servers, HP openMVS

IBM

The AIX operating system is vulnerable to the xfs issues discussed in CA-2002-34 in releases 4.3.3, 5.1.0 and 5.2.0.

IBM provides the following official fixes:

APAR number for AIX 4.3.3: IY37888 (available approx. 01/29/03)

APAR number for AIX 5.1.0: IY37886 (available approx. 04/28/03)

APAR number for AIX 5.2.0: IY37889 (available approx. 04/28/03)

A temporary patch is available through an efix package which can be found at ftp://ftp.software.ibm.com/aix/efixes/security/xfs_efix.tar.Z.

Microsoft Corporation

The component in question is not used in any Microsoft product.

NetBSD

NetBSD ships the xfs from XFree86, though its not on or used by default.

Nortel Networks

Nortel Networks products and solutions using the affected Sun Solaris operating systems may utilize the XFS daemon; it is installed and running by default on all versions of the Solaris operating system. Nortel Networks recommends either disabling this feature or, if XFS must be run, following CERT/CC's recommendations to block access to Port 7100/TCP at the network perimeter. Nortel Networks also recommends following the mitigating practices in Sun Microsystems Inc.'s Alert Notification.

For more information please contact Nortel at:

North America: 1-8004NORTEL or 1-800-466-7835

Europe, Middle East and Africa:00800 8008 9009, or +44 (0) 870 9079009

Contacts for other regions are available at www.nortelnetworks.com/help/contact/global/

OpenBSD

The xfs daemon in OpenBSD versions up to and including 2.6 is vulnerable. OpenBSD 2.7 and later is not.

Red Hat Inc.

Red Hat Linux is not affected by this vulnerability.

SGI

We're not vulnerable to this.

Sun Microsystems

The Solaris X font server (xfs(1)) is affected by VU#312313 in the following supported versions of Solaris:

Solaris 2.6

Solaris 7

Solaris 8

Solaris 9

Patches are being generated for all of the above releases. Sun will be publishing a Sun Alert for this issue at the following location shortly:

<http://sunsolve.Sun.COM/pub-cgi/retrieve.pl?doc=fsalert/48879>

The patches will be available from:

<http://sunsolve.sun.com/securitypatch>

SuSE

We are not affected.

Appendix B References

1. ISS X-Force Security Advisory: Solaris fs.auto Remote Compromise Vulnerability - <http://bvlive01.iss.net/issEn/delivery/xforce/alertdetail.jsp?oid=21541>
2. Sun Cluster 3.0 U1 Data Services Developer's Guide, Chapter 6: Sample DSDL Resource Type Implementation - <http://docs.sun.com/db/doc/806-7072/6jfvjtg11?q=xfs&a=view>
3. CERT/CC Vulnerability Note: VU#312313 - <http://www.kb.cert.org/vuls/id/312313>
4. CVE reference number CAN-2002-1317. Information available at <http://cve.mitre.org>

Internet Security Systems publicly reported this vulnerability.

Authors: Ian A. Finlay and Shawn V. Hernan

Copyright 2002 Carnegie Mellon University

Revision History

November 25, 2002: Initial release

November 25, 2002: Added vendor statement for Hewlett-Packard Company

November 25, 2002: Added vendor statement for Microsoft Corporation

December 02, 2002: Added vendor statement for SuSE

December 04, 2002: Added vendor statement for Red Hat Inc.

December 05, 2002: Revised vendor statement for OpenBSD

December 06, 2002: Revised vendor statement Hewlett-Packard Company

December 11, 2002: Added vendor statement for IBM (Note IBM provided their statement on December 5, 2002)

December 17, 2002: Added vendor statement for Nortel Networks

35 CA-2002-35: Vulnerability in RaQ Server Appliances

Original release date: December 11, 2002

Last revised: Tue Dec 17 14:43:22 EST 2002

Source: CERT/CC

A complete revision history can be found at the end of this file.

Systems Affected

- Sun Cobalt RaQ 4 Server Appliances with the Security Hardening Package installed
- Sun Cobalt RaQ 3 Server Appliances running the RaQ 4 build with the Security Hardening Package installed

Overview

A remotely exploitable vulnerability has been discovered in [Sun Cobalt RaQ Server Appliances](#) running Sun's [Security Hardening Package \(SHP\)](#). Exploitation of this vulnerability may allow remote attackers to execute arbitrary code with superuser privileges.

I. Description

Cobalt RaQ is a Sun Server Appliance. Sun provides a Security Hardening Package (SHP) for Cobalt RaQs. Although the SHP is not installed by default, many users choose to install it on their RaQ servers. For background information on the SHP, please see the [SHP RaQ 4 User Guide](#).

A vulnerability in the SHP may allow a remote attacker to execute arbitrary code on a Cobalt RaQ Server Appliance. The vulnerability occurs in a cgi script that does not properly filter input. Specifically, *overflow.cgi* does not adequately filter input destined for the *email* variable. Because of this flaw, an attacker can use a POST request to fill the *email* variable with arbitrary commands. The attacker can then call *overflow.cgi*, which will allow the command the attacker filled the *email* variable with to be executed with superuser privileges.

An exploit is publicly available and may be circulating.

Further information about this vulnerability may be found in [VU#810921](#) in the [CERT/CC Vulnerability Notes Database](#).

II. Impact

A remote attacker may be able to execute arbitrary code on a Cobalt RaQ Server Appliance with the SHP installed.

III. Solution

Apply a patch from your vendor

Appendix A contains information provided by vendors for this advisory. As vendors report new information to the CERT/CC, we will update this section and note the changes in our revision history. If a particular vendor is not listed below, we have not received their comments. Please contact your vendor directly.

Workarounds

Block access to the Cobalt RaQ administrative httpd server (typically ports 81/TCP and 444/TCP) at your network perimeter. Note that this will not protect vulnerable hosts within your network perimeter. It is important to understand your network configuration and service requirements before deciding what changes are appropriate.

Caveats

The patch supplied by Sun removes the SHP completely. If your operation requires the use of the SHP, you may need to find a suitable alternative.

Appendix A Vendor Information

Sun Microsystems

Sun confirms that a remote root exploit does affect the Sun/Cobalt RaQ4 platform if the SHP (Security Hardening Patch) patch was installed.

Sun has released a Sun Alert which describes how to remove the SHP patch:

<http://sunsolve.Sun.COM/pub-cgi/retrieve.pl?doc=fsalert/49377>

The removal patch is available from:

http://ftp.cobalt.sun.com/pub/packages/raq4/eng/RaQ4-en-Security-2.0.1-SHP_REM.pkg

Appendix B References

1. CERT/CC Vulnerability Note: VU#810921 - <http://www.kb.cert.org/vuls/id/810921>
2. Sun SHP RaQ 4 User Guide - http://www.sun.com/hardware/serverappliances/pdfs/sup-port/RaQ_4_SHP_UG.pdf
3. COBALT RaQ 4 User Manual - <http://www.sun.com/hardware/serverappliances/pdfs/manuals/manual.raq4.pdf>

grazer@digit-labs.org publicly reported this vulnerability.

Author: Ian A. Finlay

Copyright 2002 Carnegie Mellon University

Revision History

December 11, 2002: Initial release

December 16, 2002: Added information stating RaQ 3 Server Appliances are vulnerable as well (with SHP installed)

December 16, 2002: Revised systems affected section

36 CA-2002-36: CERT® Advisory CA-2002-36 Multiple Vulnerabilities in SSH Implementations

Original issue date: December 16, 2002

Last revised: May 5, 2003

Source: CERT/CC

A complete revision history is at the end of this file.

Systems Affected

Secure shell (SSH) protocol implementations in SSH clients and servers from multiple vendors

Overview

Multiple vendors' implementations of the secure shell (SSH) transport layer protocol contain vulnerabilities that could allow a remote attacker to execute arbitrary code with the privileges of the SSH process or cause a denial of service. The vulnerabilities affect SSH clients and servers, and they occur before user authentication takes place.

Summary vendor information can be found in the [Systems Affected](#) section of VU#389665.

I. Description

The SSH protocol enables a secure communications channel from a client to a server. From the IETF draft *SSH Transport Layer Protocol*:

The SSH transport layer is a secure low level transport protocol. It provides strong encryption, cryptographic host authentication, and integrity protection.... Key exchange method, public key algorithm, symmetric encryption algorithm, message authentication algorithm, and hash algorithm are all negotiated.

[Rapid7](#) has developed a suite (SSHredder) of test cases that examine the connection initialization, key exchange, and negotiation phase (KEX, KEXINIT) of the SSH transport layer protocol. The suite tests the way an SSH transport layer implementation handles invalid or incorrect packet and string lengths, padding and padding length, malformed strings, and invalid algorithms.

The test suite has demonstrated a number of vulnerabilities in different vendors' SSH products. These vulnerabilities include buffer overflows, and they occur before any user authentication takes place. SSHredder was primarily designed to test key exchange and other processes that are specific to version 2 of the SSH protocol; however, certain classes of tests are also applicable to version 1.

Further information about this set of vulnerabilities may be found in Vulnerability Note [VU#389665](#).

Rapid7 has published a detailed advisory ([R7-0009](#)) and the [SSHredder](#) test suite.

Common Vulnerabilities and Exposures ([CVE](#)) has assigned the following candidate numbers for several classes of tests performed by SSHredder:

- [CAN-2002-1357](#) - incorrect field lengths
- [CAN-2002-1358](#) - lists with empty elements or multiple separators
- [CAN-2002-1359](#) - "classic" buffer overflows
- [CAN-2002-1360](#) - null characters in strings

II. Impact

The impact will vary for different vulnerabilities and products, but in severe cases, remote attackers could execute arbitrary code with the privileges of the SSH process. Both SSH clients and servers are affected, since both implement the SSH transport layer protocol. On Microsoft Windows systems, SSH servers commonly run with SYSTEM privileges, and on UNIX systems, SSH daemons typically run with root privileges. In the case of SSH clients, any attacker-supplied code would run with at least the privileges of the user who started the client program. Additional privileges may be afforded to an attacker when the SSH client is setuid or setgid to a more privileged user, such as root. Attackers could also crash a vulnerable SSH process, causing a denial of service.

III. Solution

Apply a patch or upgrade

Apply the appropriate patch or upgrade as specified by your vendor. See [Appendix A](#), below and the [Systems Affected](#) section of VU#389665 for further information.

Restrict access

Limit access to SSH servers to trusted hosts and networks using firewalls or other packet-filtering systems. Some SSH servers may have the ability to restrict access based on IP addresses, or similar effects may be achieved by using TCP wrappers or other related technology.

SSH clients can reduce the risk of attacks by only connecting to trusted servers by IP address.

While these workarounds will not prevent exploitation of these vulnerabilities, they will make attacks somewhat more difficult, in part by limiting the number of potential sources of attacks.

Appendix A Vendor Information

This appendix contains information provided by vendors. When vendors report new information, this section is updated and the changes are noted in the revision history. If a vendor is not listed below, we have not received their comments. The [Systems Affected](#) section of VU#389665 contains additional vendor status information.

Alcatel

Following CERT advisory CA-2002-36 on security vulnerabilities in the SSH implementations, Alcatel has conducted an immediate assessment to determine any impact this may have on our portfolio. A first analysis showed that various Alcatel products were affected: namely the 6600, 7000 and 8000 OmniSwitches running AOS 5.1.3 and for which corrections had been made available to customers. This issue has now been fixed both in a AOS 5.1.3 maintenance release and in AOS 5.1.4. The security of our customers' networks is of highest priority for Alcatel. Therefore we continue to test our product portfolio against potential SSH security vulnerabilities and will provide updates if necessary.

Apple Computer Inc.

Apple: Mac OS X and Mac OS X Server do not contain the vulnerabilities described in this report.

Cisco Systems, Inc.

Cisco Systems has several products that are vulnerable to the attacks posed by the SSHredder test suite. Complete details are available at <http://www.cisco.com/warp/public/707/ssh-packet-suite-vuln.shtml>.

Based on initial testing and evaluation of this vulnerability, earlier versions of this advisory listed Cisco Systems as "Not Vulnerable." Upon additional internal testing it was determined that some Cisco products were indeed vulnerable.

Cray Inc.

Cray Inc. supports the OpenSSH product through their Cray Open Software (COS) package. COS 3.3, available the end of December 2002, is not vulnerable. If a site is concerned, they can contact their local Cray representative to obtain an early copy of the OpenSSH contained in COS 3.3.

cryptlib

From testing against the SSHredder data the invalid packets are being caught and rejected by cryptlib's packet validity-checking code, making it not vulnerable to the problem.

F-Secure

F-Secure SSH products are not exploitable via these attacks. While F-Secure SSH versions 3.1.0 build 11 and earlier crash on these malicious packets, we did not find ways to exploit this to gain unauthorized access or to run arbitrary code. Furthermore, the crash occurs in a forked process so the denial of service attacks are not possible.

Fujitsu

Fujitsu's UXP/V OS is not vulnerable because it does not support SSH.

Hewlett-Packard

SOURCE: Hewlett-Packard Company

HP Tru64 UNIX V5.1a or HP OpenVMS systems using SSH V2.4.1 should upgrade to SSH V3.2.

HP has investigated this report and find that our implementations within HP-UX are not vulnerable.

IBM

IBM's AIX is not vulnerable to the issues discussed in CERT CA-2002-36.

Juniper Networks

Juniper Networks has determined that the software on the ERX router platforms is susceptible to this vulnerability. Patches for all supported releases are now available to resolve the vulnerability. Customers should contact the Juniper Networks Technical Assistance Center to obtain the latest patch.

Initial testing of the JUNOS software on Juniper's M-, T-, and J-series routers has not revealed any susceptibility to this vulnerability. Juniper will continue testing, and if any problems are found, corrective action will be taken.

The Juniper G-series Cable Modem Termination Systems are not susceptible to this vulnerability.

lsh

I've now tried the testsuite with the latest stable release of lsh, lsh-1.4.2. Both the client and the server seem NOT VULNERABLE.

NetScreen Technologies Inc.

Tested latest versions. Not Vulnerable.

Nortel Networks

The following Nortel Networks products are being assessed to determine whether they are potentially affected by the vulnerabilities identified in CERT Advisory CA-2002-36: Shasta Broadband Service Node and Shasta Service Creation System.

Passport 8000 Series Software is potentially affected; this issue will be addressed in the next maintenance releases

3.3.2.0, for version 3.3, scheduled for availability January 24th, 2003.

3.2.4, for version 3.2, scheduled for availability in Mid March 2003 (target)

Releases before 3.2.1 are not affected.
A product bulletin will be issued shortly.

STORM is potentially affected; a product bulletin will be issued shortly and this issue will be addressed in the next Maintenance Release scheduled for availability in March, 2003.

Other Nortel Networks products implementing SSH are not affected by the vulnerabilities identified in CERT Advisory CA-2002-36.

For more information please contact Nortel at:

North America: 1-8004NORTEL or 1-800-466-7835

Europe, Middle East and Africa: 00800 8008 9009, or +44 (0) 870 907 9009

Contacts for other regions are available at <<http://www.nortelnetworks.com/help/contact/global/>>

OpenSSH

From my testing it seems that the current version of OpenSSH (3.5) is not vulnerable to these problems, and some limited testing shows that no version of OpenSSH is vulnerable.

Pragma Systems, Inc.

December 16, 2002

Rapid 7 and CERT Coordination Center Vulnerability report VU#389665

Pragma Systems Inc. of Austin, Texas, USA, was notified regarding a possible vulnerability with Version 2.0 of Pragma SecureShell. Pragma Systems tested Pragma SecureShell 2.0 and the upcoming new Version 3.0, and found that the attacks did cause a memory access protection fault on Microsoft platforms.

After research, Pragma Systems corrected the problem. The correction of the problem leads us to believe that any attack would not cause a Denial of Service, or the ability of random code to run on the server.

The problem is corrected in Pragma SecureShell Version 3.0. Any customers with concerns regarding this vulnerability report should contact Pragma Systems, Inc at support@pragmasys.com for information on obtaining an upgrade free of charge. Pragma's web site is located at www.pragmasys.com and the company can be reached at 1-512-219-7270.

PuTTY

PuTTY versions 0.53 and earlier are vulnerable to a buffer overrun discovered by SSHredder. Version 0.53b fixes this vulnerability.

Riverstone Networks

Riverstone's implementation of SSH is based on OpenSSH, which is not vulnerable to any of the particular tests that are run by the SSHredder test suite. However, while running the test suite under certain conditions the router can experience a problem causing it to reload.

For more details, please see http://www.riverstonenet.com/support/support_security.shtml and the security advisory at <http://www.riverstonenet.com/support/tb0239-9.shtml>.

SSH Communications Security

With SSH Secure Shell the worst case effect of the vulnerability is a denial of service (DoS) for a single child-server (connection). This cannot be exploited to gain access to the host and this does not affect the parent server in any way nor does it hinder the server's ability to receive new connections - it only affects the child server that is handling connections to the malicious client, or a client application that is connecting to a malicious server. No arbitrary code can be executed.

Sun Microsystems Inc.

The version of Secure Shell (SSH) shipped with Solaris 9 is not affected by the issues described in CERT VU#389665.

VanDyke Software

From our testing it seems that the current versions of VanDyke's Secure Shell implementations are not vulnerable to these problems, and some limited testing shows that no prior VanDyke Secure Shell implementations are vulnerable.

Official Releases Tested:

Server:

VShell 2.1.1 October 15, 2002

Clients:

SecureCRT 4.0.2 December 3, 2002

SecureFX 2.1.1 November 7, 2002

Entunnel 1.0.1 October 15, 2002

Older Releases Tested:

Servers:

VShell 2.0.3 May 28, 2002

VShell 1.2.4 May 28, 2002

Clients:

SecureCRT 3.4.7 November 7, 2002

Xerox

A response to this advisory is available from our web site:

<http://www.xerox.com/security>.

Appendix B References

- CERT/CC Vulnerability Note: VU#389665 - <http://www.kb.cert.org/vuls/id/389665>
- Rapid 7 Advisory: R7-0009 - <http://www.rapid7.com/advisories/R7-0009.txt>
- Rapid 7 SSHredder test suite - <http://www.rapid7.com/perl/DownloadRequest.pl?PackageChoice=666>
- IETF Draft: SSH Transport Layer Protocol - <http://www.ietf.org/internet-drafts/draft-ietf-secsh-transport-15.txt>
- IETF Draft: SSH Protocol Architecture - <http://www.ietf.org/internet-drafts/draft-ietf-secsh-architecture-13.txt>
- Privilege Separated OpenSSH - <http://www.citi.umich.edu/u/provos/ssh/privsep.html>

The CERT Coordination Center thanks Rapid7 for researching and reporting these vulnerabilities.

Author: Art Manion

This document is available from: <http://www.cert.org/advisories/CA-2002-36.html>

CERT/CC Contact Information

Email: cert@cert.org

Phone: +1 412-268-7090 (24-hour hotline)

Fax: +1 412-268-6989

Postal address:

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
U.S.A.

CERT/CC personnel answer the hotline 08:00-17:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

Using encryption

We strongly urge you to encrypt sensitive information sent by email. Our public PGP key is available from

- http://www.cert.org/CERT_PGP.key

If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

CERT publications and other security information are available from our web site

- <http://www.cert.org/>

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

NO WARRANTY

Any material furnished by Carnegie Mellon University and the Software Engineering Institute is furnished on an "as is" basis. Carnegie Mellon University makes no warranties of any kind, either expressed or implied as to any matter including, but not limited to, warranty of fitness for a particular purpose or merchantability, exclusivity or results obtained from use of the material. Carnegie Mellon University does not make any warranty of any kind with respect to freedom from patent, trademark, or copyright infringement.

Conditions for use, disclaimers, and sponsorship information

Copyright 2002 Carnegie Mellon University

Revision History

December 16, 2002: Initial release, clarified setuid/setgid SSH client impact, updated IBM statement
December 17, 2002: Added VanDyke statement, updated SSH.com statement, removed PuTTY statement, added DoS impact, fixed Pragma link
December 18, 2002: Updated Cisco statement, added HP statement
December 20, 2002: Updated Cisco statement, added Sun statement, added Apple statement, added vendor information link to Overview
January 2, 2003: Added Riverstone statement.
January 6, 2003: Added Juniper statement
January 7, 2003: (Re-)added PuTTY statement
January 9, 2003: Updated Juniper statement
January 20, 2003: Added Nortel statement
February 25, 2003: Added Alcatel and Xerox statements
March 11, 2003: Added cryptlib statement
May 5, 2003: Updated Alcatel statement

37 CA-2002-37: CERT® Advisory CA-2002-37 Buffer Overflow in Microsoft Windows Shell

Original release date: December 19, 2002

Last revised: --

Source: CERT/CC

A complete revision history can be found at the end of this file.

Systems Affected

- All versions of Microsoft Windows XP

Overview

A buffer overflow vulnerability exists in the Microsoft Windows Shell. An attacker can exploit this vulnerability by enticing a victim to read a malicious email message, visit a malicious web page, or browse to a folder containing a malicious .MP3 or .WMA file. The attacker can then execute arbitrary code with the privileges of the victim.

I. Description

The Microsoft Windows Shell provides the basic human-computer interface for Windows systems. Browsing local and remote folders, running wizards, and performing configuration tasks are examples of operations utilizing the Windows Shell. Microsoft describes the Windows Shell as follows:

The Windows Shell is responsible for providing the basic framework of the Windows user interface experience. It is most familiar to users as the Windows Desktop, but also provides a variety of other functions to help define the user's computing session, including organizing files and folders, and providing the means to start applications.

A vulnerability exists in the Windows Shell function used to extract attribute information from audio files. This function is invoked automatically when a user browses to a folder containing .MP3 or .WMA files. Further information about this vulnerability can be found in the following documents:

- [Foundstone Research Labs Advisory FS2002-11](#)
[Microsoft Security Bulletin MS02-072](#)
[CERT/CC Vulnerability Note VU#591890](#)

A CVE candidate [CAN-2002-1327](#) has been assigned as well.

II. Impact

An attacker can either execute arbitrary code (which would run with the privileges of the victim) or crash the Windows Shell.

III. Solution

Apply a patch from your vendor

[Appendix A](#) contains information provided by vendors for this advisory. As vendors report new information to the CERT/CC, we will update this section and note the changes in our revision history. If a particular vendor is not listed below, we have not received their comments. Please contact your vendor directly.

Note that Microsoft is actively deploying the patch for this vulnerability via [Windows Update](#).

Appendix A Vendor Information

[Microsoft Corporation](#)

Please see <http://www.microsoft.com/technet/treeview/?url=/technet/security/bulletin/MS02-072.asp>.

Appendix B References

- Foundstone Research Labs Advisory FS2002-11 - <http://www.foundstone.com/knowledge/randd-advisories-display.html?id=339>
- Microsoft Security Bulletin MS02-072 - <http://www.microsoft.com/technet/treeview/?url=/technet/security/bulletin/MS02-072.asp>
- CERT/CC Vulnerability Note VU#591890 - <http://www.kb.cert.org/vuls/id/591890>
- CVE CAN-2002-1327 - <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-1327>

[Foundstone Research Labs](#) discovered this vulnerability.

Author: [Ian A. Finlay](#)

This document is available from: <http://www.cert.org/advisories/CA-2002-37.html>

CERT/CC Contact Information

Email: cert@cert.org

Phone: +1 412-268-7090 (24-hour hotline)

Fax: +1 412-268-6989

Postal address:

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
U.S.A.

CERT/CC personnel answer the hotline 08:00-17:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

Using encryption

We strongly urge you to encrypt sensitive information sent by email. Our public PGP key is available from

- http://www.cert.org/CERT_PGP.key

If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

CERT publications and other security information are available from our web site

- <http://www.cert.org/>

To subscribe to the CERT mailing list for advisories and bulletins, send email to major-domo@cert.org. Please include in the body of your message

`subscribe cert-advisory`

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

NO WARRANTY

Any material furnished by Carnegie Mellon University and the Software Engineering Institute is furnished on an "as is" basis. Carnegie Mellon University makes no warranties of any kind, either expressed or implied as to any matter including, but not limited to, warranty of fitness for a particular purpose or merchantability, exclusivity or results obtained from use of the material. Carnegie Mellon University does not make any warranty of any kind with respect to freedom from patent, trademark, or copyright infringement.

Conditions for use, disclaimers, and sponsorship information

Copyright 2002 Carnegie Mellon University

Revision History

December 19, 2002: Initial release