Software Engineering Institute
Carnegie Mellon University

1995 CERT Advisories

CERT Division

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

http://www.sei.cmu.edu

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-1995-01: IP Spoofing Attacks and Hijacked Terminal Connections

Original issue date: January 23, 1995
Last revised: September 23, 1997
Updated Copyright Statement

A complete revision history is at the end of this file. **The IP Spoofing portion of this advisory has been superseded by CA-96.21**

The CERT Coordination Center has received reports of attacks in which intruders create packets with spoofed source IP addresses. These attacks exploit applications that use authentication based on IP addresses. This exploitation leads to user and possibly root access on the targeted system. Note that this attack does not involve source routing. Recommended solutions are described in Section III below.

In the current attack pattern, intruders may dynamically modify the kernel of a Sun 4.1.X system once root access is attained. In this attack, which is separate from the IP spoofing attack, intruders use a tool to take control of any open terminal or login session from users on the system. Note that although the tool is currently being used primarily on SunOS 4.1.x systems, the system features that make this attack possible are not unique to SunOS.

We will update this advisory as we receive additional information. Please check advisory files regularly for updates that relate to your site.

I. Description

This description summarizes both the IP spoofing technique that can lead to root access on a system and the tool that intruders are using to take over open terminal and login connections after they get root access. We are currently seeing attacks in which intruders combine IP spoofing with use of the tool. However, these are two separate actions. Intruders can use IP spoofing to gain root access for any purpose; similarly, they can highjack terminal connections regardless of their method of gaining root access.

IP spoofing
To gain access, intruders create packets with spoofed source IP addresses. This exploits applications that use authentication based on IP addresses and leads to unauthorized user and possibly root access on the targeted system. It is possible to route packets through filtering-router firewalls if they are not configured to filter incoming packets whose source address is in the local domain. It is important to note that the described attack is possible even if no reply packets can reach the attacker.

Examples of configurations that are potentially vulnerable include

- routers to external networks that support multiple internal interfaces

- routers with two interfaces that support subnetting on the internal network
- proxy firewalls where the proxy applications use the source IP address for authentication

The IP spoofing attacks we are currently seeing are similar to those described in two papers: 1) "Security Problems in the TCP/IP Protocol Suite" by Steve Bellovin, published in _Computer Communication Review_ vol. 19, no. 2 (April 1989) pages 32-48; 2) "A Weakness in the 4.2BSD Unix TCP/IP Software" by Robert T. Morris. Both papers are available by anonymous FTP from ftp://ftp.research.att.com/dist/internet_security.

Bellovin paper: ipext.ps.Z
Morris paper: 117.ps.Z

Services that are vulnerable to the IP spoofing attack include

SunRPC & NFS
BSD UNIX "r" commands
anything wrapped by the tcp daemon wrappers - site dependent; check your configuration
X windows
other applications that use source IP addresses for authentication

Hijacking tool
Once the intruders have root access on a system, they can use a tool to dynamically modify the UNIX kernel. This modification allows them to hijack existing terminal and login connections from any user on the system.

In taking over the existing connections, intruders can bypass one-time passwords and other strong authentication schemes by tapping the connection after the authentication is complete. For example, a legitimate user connects to a remote site through a login or terminal session; the intruder hijacks the connection after the user has completed the authentication to the remote location; the remote site is now compromised. (See Section I for examples of vulnerable configurations.)

Currently, the tool is used primarily on SunOS 4.1.x systems. However, the system features that make this attack possible are not unique to SunOS.

The CERT Coordination Center has been informed that any services that use Kerberos for authentication should not be vulnerable to an IP spoofing attack. For more information about Kerberos, see ftp://rtfm.mit.edu/pub/usenet/news.answers/kerberos-faq.

Also note that the information and solution described in this advisory does not address the issue of mobile IP spoofing.

II. Impact

Current intruder activity in spoofing source IP addresses can lead to unauthorized remote root access to systems behind a filtering-router firewall.

After gaining root access and taking over existing terminal and login connections, intruders can gain access to remote hosts.

III. Solutions

A. Detection

IP spoofing
If you monitor packets using network-monitoring software such as netlog, look for a packet on your external interface that has both its source and destination IP addresses in your local domain. If you find one, you are currently under attack. Netlog is available by anonymous FTP from
ftp://net.tamu.edu/pub/security/TAMU/netlog-1.2.tar.gz
MD5 checksum: 1dd62e7e96192456e8c75047c38e994b

Another way to detect IP spoofing is to compare the process accounting logs between systems on your internal network. If the IP spoofing attack has succeeded on one of your systems, you may get a log entry on the victim machine showing a remote access; on the apparent source machine, there will be no corresponding entry for initiating that remote access.

Hijacking tool
When the intruder attaches to an existing terminal or login connection, users may detect unusual activity, such as commands appearing on their terminal that they did not type or a blank window that will no longer respond to their commands. Encourage your users to inform you of any such activity. In addition, pay particular attention to connections that have been idle for a long time.

Once the attack is completed, it is difficult to detect. However, the intruders may leave remnants of their tools. For example, you may find a kernel streams module designed to tap into existing TCP connections.

B. Prevention

IP spoofing
The best method of preventing the IP spoofing problem is to install a filtering router that restricts the input to your external interface (known as an input filter) by not allowing a packet through if it has a source address from your internal network. In addition, you should filter outgoing packets that have a source address different from your internal network in order to prevent a source IP spoofing attack originating from your site.

The following vendors have reported support for this feature:

Bay Networks/Wellfleet routers, version 5 and later
Cabletron - LAN Secure
Cisco - RIS software all releases of version 9.21 and later
Livingston - all versions

3COM, Cisco Systems, and Morning Star Technologies have provided detailed information, which you can find in Appendix A of this advisory.

If you need more information about your router or about firewalls, please contact your vendor directly.

If your vendor's router does not support filtering on the inbound side of the interface or if there will be a delay in incorporating the feature into your system, you may filter the spoofed IP packets by using a second router between your external interface and your outside connection. Configure this router to block, on the outgoing interface connected to your original router, all packets that have a source address in your internal network. For this purpose, you can use a filtering router or a UNIX system with two interfaces that supports packet filtering.

NOTE: Disabling source routing at the router does not protect you from this attack, but it is still good security practice to do so.

Additional information about protecting yourself from IP spoofing attacks is in Updates section at the end of this file; these updates were added after the initial release of the advisory.

Hijacking tool

There is no specific way to prevent use of the tool other than preventing intruders from gaining root access in the first place. If you have experienced a root compromise, see Section C for general instructions on how to recover.

C. Recovery from a UNIX root compromise

1. Disconnect from the network or operate the system in single-user mode during the recovery. This will keep users and intruders from accessing the system.
2. Verify system binaries and configuration files against the vendor's media (do not rely on timestamp information to provide an indication of modification). Do not trust any verification tool such as *cmp(1)* located on the compromised system as it, too, may have been modified by the intruder. In addition, do not trust the results of the standard UNIX *sum(1)* program as we have seen intruders modify system files in such a way that the checksums remain the same. Replace any modified files from the vendor's media, not from backups.

   -- or --

   Reload your system from the vendor's media.

3. Search the system for new or modified setuid root files.

4.
   ```
   find / -user root -perm -4000 -print
   ```

   If you are using NFS or AFS file systems, use ncheck to search the local file systems.

   ```
   ncheck -s /dev/sd0a
   ```

5. Change the password on all accounts.
6. Don't trust your backups for reloading any file used by root. You do not want to re-introduce files altered by an intruder.

Appendix A: Vendor Information

3COM

The following information has been provided by 3COM for their customers.

Begin Text Provided by 3COM

The following examples illustrate how NETBuilder software can be configured to support the CERT Advisory recommendations. Each of these examples assumes that the value of the -IP FilterDefAction parameter is configured to Forward.

Example 1:

This example illustrates a two-router solution where the internal network is configured with non-contiguous IP network numbers. The filters are installed on the border router which can only have two interfaces. In a two-port router, an output filter on one port is equivalent to an input filter on the other port. Please refer to Figure 1:

Figure 1: Non-Contiguous IP Networks

```
                         |
            | Border |   |   |Internal|--- 10.0.0.0
Outside  --| Router |---|---| Router |
                         |   |        |--- 20.0.0.0
                         |
                      30.0.0.0
```

The border router is configured with the following filters:

```
ADD -IP FilterAddrs 10.0.0.0/0.255.255.255 >
           10.0.0.0/0.255.255.255 Discard
ADD -IP FilterAddrs 20.0.0.0/0.255.255.255 >
           20.0.0.0/0.255.255.255 Discard
ADD -IP FilterAddrs 30.0.0.0/0.255.255.255 >
```

```
           30.0.0.0/0.255.255.255 Discard

ADD -IP FilterAddrs 10.0.0.0/0.255.255.255 <>

           20.0.0.0/0.255.255.255 Discard

ADD -IP FilterAddrs 10.0.0.0/0.255.255.255 <>

           30.0.0.0/0.255.255.255 Discard

ADD -IP FilterAddrs 20.0.0.0/0.255.255.255 <>

           30.0.0.0/0.255.255.255 Discard
```

This configuration prevents the external attack and allows the internal router to route traffic between networks 10.0.0.0, 20.0.0.0, and 30.0.0.0. This configuration also works for the cascade topology shown in Figure 2.

Figure 2: Non-Contiguous IP Networks (alternate topology)

```
                         |                |

            | Border |   |   |Internal|   |   |Internal|

Outside ---| Router |---|---| Router |---|---| Router |--- 10.0.0.0

                         |                |

                         |                |

                     30.0.0.0         20.0.0.0
```

Example 2:

The second example illustrates a two-router solution when the internal network is configured with multiple subnets of the Class B network address - 130.5.0.0. The subnet mask is 255.255.255.0. Please refer to Figure 3.

Figure 3: Subnets on the Internal Network

```
                         |

            | Border |   |   |Internal|--- 130.5.2.0

Outside  --| Router |---|---| Router |

                         |   |        |--- 130.5.3.0

                         |

                     130.5.1.0    Subnet Mask = 255.255.255.0
```

The border router is configured with the following filter:

```
ADD -IP FilterAddrs 130.5.0.0/0.0.255.255 >

          130.5.0.0/0.0.255.255 Discard
```

This configuration prevents the external attack and allows the internal route to route traffic between all subnetworks of 130.5.0.0. In this example, a single filter can protect multiple subnets.

Example 3:

The final example illustrates a two-router solution when the internal network is configured with contiguous IP network numbers. Assume the service provider has provided the subscriber with the CIDR block 200.5.0.0/255.255.0.0. Please refer to Figure 4:

Figure 4: Multiple Contiguous IP Networks

```
                         |

            | Border |   |   |Internal|---  200.5.2.0

Outside  --| Router |---|---| Router |

                         |   |        |---  200.5.3.0

                         |

                      200.5.1.0    CIDR Mask = 255.255.0.0
```

The border router is configured with the following filter:

```
ADD -IP FilterAddrs 200.5.0.0/0.0.255.255 >

           200.5.0.0/0.0.255.255 Discard
```

This configuration prevents the external attack and allows the internal router to route traffic between supernets of 200.5.0.0/255.255.0.0. In this example, a single filter can protect multiple contiguous IP networks numbers assigned as a CIDR block.

End Text Provided by 3COM

Cisco Systems

The following information has been provided by Cisco Systems for their customers.

Begin Text Provided by Cisco

The defense is to set up your internet firewall router to deny packets from OUTSIDE your network that claim to have a source address INSIDE your network.

example configuration:

```
access-list 101 deny ip 131.108.0.0 0.0.255.255 0.0.0.0
255.255.255.255
```

```
access-list 101 deny ip 198.92.93.0 0.0.0.255 0.0.0.0
255.255.255.255
```

```
[..rest of your firewall goes here..]
```

and so on, where access list 101 describes all possible source addresses on YOUR network. The example above describes a network with internal source addresses of 131.108.x.x and 198.92.93.x

Note: If you use only the two line example described above without any other access-list commands, ALL TRAFFIC will be stopped on your interface since the implicit action of an unmatched access-list is to deny packets.

If you only want source address spoofing protection and nothing else, add the line

```
access-list 101 permit ip 0.0.0.0 255.255.255.255 0.0.0.0
255.255.255.255
```

to the end of the earlier example. This is NOT an optimal solution since there are many other possible attacks barring the IP spoofing fixed here.

There are articles on this topic on the CIO information service and various USENET mailing lists. You can telnet to cio.cisco.com or point your WWW browser at http://www.cisco.com.

Anyway! Once you have defined an appropriate access list you can apply them to the vulnerable interfaces.

Assuming your interface serial 0 faces the Internet:

```
interface serial 0
```

```
description interface facing the big, bad Internet
```

ip access-group 101 in for a router running 9.21 or later.

If you DO NOT have 9.21, an upgrade is NOT required if your internet firewall is a two port router (which it should be). Simply apply access-list 101 as described above to the LAN interface and not the serial interface.

example:

```
interface ethernet 0
```

```
description LAN port on my internet router
```

```
ip access-group 101
```

The essence of this defense is that any packets coming from the internet that claim to be from your network are tossed, thereby preventing the style of attack described below.

Also, for good measure, ALL INTERNET FIREWALLS should have the global command

```
no ip source-route
```

Which helps prevent other forms of spoofing attack from outside.

For further discussion of sequence number guessing attacks, see papers by Morris and also Bellovin in

ftp://ftp.research.att.com/dist/internet_security/117.ps.Z

ftp://ftp.research.att.com/dist/internet_security/ipext.ps.Z

End Text Provided by Cisco

Morning Star Technologies, Inc.

The following information has been provided by Morning Star Technologies for their customers.

Begin Text Provided by Morning Star

TO ALL USERS OF MORNING STAR PRODUCTS:

Here is how to configure your Internet interface to prevent such

attacks:

1) Locate the packet filter file controlling your interface to the Internet. For users of Morning Star PPP, this will usually be /etc/ppp/Filter, /usr/etc/ppp/Filter, or /usr/lib/ppp/Filter.

Users of Express routers should look in the file called Filter.

Check your pppd (or frd for frame relay users) command line for a possibly different filter filename, or look for `ifconfig [interface] filter [filename]' commands in your Express router's rc.boot file.

2) Within the packet filter file, locate the individual filter specification used by your Internet connection. It will begin with either the hostname or IP address of the remote side of a PPP connection, the local hostname or IP address of a frame relay, Ethernet,

or RF modem connection, or the special keyword `default' for any type of connection.

3) Within the appropriate filter specification, locate the `pass' filter.

4) Add the following line to the beginning of the pass filter:

```
!ip_opt=srcrt
```

This will cause all transmitted or received IP packets with Source Routing options to be discarded.

5) Determine the IP network number or numbers of your internal network or networks. Insert a set of lines similar to the following pair following the source route rule described in step 4) above for each internal network number.

```
!recv/src/[network-number]

!send/dst/[network-number]
```

This will block all received packets containing a source IP address in your internal network, and will block the transmission of all packets containing a destination IP address in your internal network. For example, we have Class B network

137.175, so our Filter file contains

```
!ip_opt=srcrt

!recv/src/137.175.0.0

!send/dst/137.175.0.0
```

If you don't have a whole IP network, you'll also need to specify a netmask. For example, an organization that has both the Class C network 192.1.1.0 and the Class-C-sized 10.1.220.0 segment of the Class A net 10 would add these lines

```
!ip_opt=srcrt

!recv/src/192.1.1.0

!send/dst/192.1.1.0

!recv/src/10.1.220.0/255.255.255.0

!send/dst/10.1.220.0/255.255.255.0
```

FURTHER NOTE:

Do not configure any of your systems to trust any of the Unix `r' commands (rlogin, rsh, etc.) from any machine outside your firewall. Such systems can be spoofed as easily as internal machines, but spoofed packets cannot be detected at your firewall.

GETTING MORE HELP:

If you need any help with these modifications, call our customer support hotline at +1 800 558 7827 or send us e-mail at support@MorningStar.Com. When sending e-mail, please include the phrase CERT SECURITY PROBLEM in your Subject: header. We will provide assistance with this to all Morning Star customers, even for those without current customer support agreements. If you do not have a current support agreement, use the phrase `CERT SECURITY PROBLEM' when asked for your customer support number.

End Text Provided by Morning Star

The CERT Coordination Center thanks Eric Allman, Steve Bellovin, Keith Bostic, Bill Cheswick, Mike Karels, and Tsutomu Shimomura for contributing to our understanding of these problems and their solutions.

UPDATES

Additional steps you can take to address IP spoofing:

For IP spoofing to be successful, intruders rely on two machines to trust each other through the use of the .rhosts file or the /etc/hosts.equiv file. By exploiting applications that use authentication based on IP addresses (e.g., rsh and rlogin), intruders can gain user or root access on targeted hosts.

We suggest that you use TCP wrappers to allow access from only a select few machines. Although this is not a complete solution, it does reduce your susceptibility to attack. Alternatively, change the configuration of your Internet gateway so that rlogin and rsh from the Internet to hosts in your domain are blocked. If that is not possible, disable the rlogin and rsh services on all of your hosts.

Some sites have turned off source routing thinking that this would prevent IP spoofing attacks. This is NOT the case. Although we encourage sites to turn off source routing this does not prevent IP spoofing attacks. To prevent such attacks it is necessary to undertake packet filtering as described in the advisory.

In addition to the attacks described in this advisory, we are now seeing attacks in which intruders gain access to a site using loopback IP addresses rather than IP addresses particular to that site.

We recommend that in addition to the packet filtering suggestions described in Section III B of the advisory, you configure the filtering router to filter inbound packets in the following IP ranges:

127.0.0.0	-	127.255.255.255	(loopback)
10.0.0.0	-	10.255.255.255	(reserved)
172.16.0.0	-	172.31.255.255	(reserved)
192.168.0.0	-	192.168.255.255	(reserved)

Finally, we encourage you to consider using network monitoring tools to check for signs of IP spoofing attacks. Argus is a network monitoring tool that uses a client-server model to capture data and associate it into "transactions." The tool provides network-level auditing; it can verify compliance to a router configuration file, and information is easily adapted to protocol analysis, intrusion detections, and other security needs. Argus is available from ftp://ftp.net.cmu.edu/pub/argus-1.5.

Revision History

Sep. 23, 1997	Update Copyright statement
Dec. 19, 1996	Updates section - reminder
Sep. 24, 1996	Supersession statement modified
Sep. 19, 1996	Superseded by CA-96.21 [IP spoofing portion only]
Aug. 30, 1996	Information previously in the README was inserted into the advisory. Appendix A - added vendor information as it was received: Cisco Systems, Morning Star Technologies, and 3COM.
May 10, 1996	Updates section - added pointer to the Argus tool.
Aug. 04, 1995	Updates section - added more information on IP Spoofing and recommendations for detecting such

```
               activity.
Aug. 04, 1995  Sec. I - added notes about Kerberos and mobile IP
               spoofing.
```

2 CA-1995-02: Vulnerabilities in /bin/mail

Original issue date: January 26, 1995
Last revised: September 23, 1997
Updated Copyright statement

A complete revision history is at the end of this file. **This advisory supersedes CA-91.01a and CA-91.13.**

There are vulnerabilities in some versions of /bin/mail. Section III below provides vendor-specific information and an alternative to /bin/mail.

We will update this advisory as we receive additional information. Please check advisory files regularly for updates that relate to your site.

I. Description

Some versions of /bin/mail based on BSD 4.3 UNIX are vulnerable because of timing windows in the way /bin/mail uses publicly writable directories.

II. Impact

Local users (users that have an account on the system) can create or modify root-owned files on the system and can thereby gain unauthorized root access.

III. Solutions

Either install a patch from your vendor or replace /bin/mail with mail.local.

A. Obtain the appropriate patch from your vendor and install it according to the instructions included with the patch.

Below is a summary of the vendors listed in Appendix A of this advisory and the information they have provided. If your vendor's name is not on this list, please contact the vendor directly.

Vendor or Source	Status
Apple Computer, Inc.	not vulnerable
Berkeley SW Design, Inc. (BSDI)	not vulnerable
Data General Corp.	not vulnerable
Digital Equipment Corp.	vulnerable, patches available

Free BSD	not vulnerable
Harris	not vulnerable
IBM	not vulnerable
NetBSD	not vulnerable
NeXT, Inc.	not vulnerable
Pyramid	not vulnerable
The Santa Cruz Operation (SCO)	see note in Appendix A
Solbourne (Grumman)	vulnerable - contact vendor
Sun Microsystems, Inc.	SunOS 4.x vulnerable, patches available, patch revisions coming soon
	Solaris 2.x not vulnerable

B. Replace /bin/mail with mail.local.

If you cannot obtain a vendor-supplied replacement for /bin/mail, the CERT Coordination Center recommends using mail.local as a replacement for /bin/mail.

Although the current version of mail.local is not a perfect solution, it addresses the vulnerabilities currently being exploited in /bin/mail.

mail.local is now provided with the lastest version of sendmail. That version can be found at ftp://ftp.cert.org/pub/tools/sendmail/sendmail-latest*.

The original version of mail.local has been tested on SunOS 4.1 and Ultrix 4.X systems.

Mail.local.c for BSD 4.3 systems, along with a README file containing installation instructions, can be found on the anonymous FTP servers listed below.

Location

ftp://ftp.cert.org/pub/tools/mail.local/mail.local.c
MD5 c0d64e740b42f6dc5cc54a2bc37c31b0

ftp://coast.cs.purdue.edu/pub/tools/unix/mail.local/mail.local.c
MD5 c0d64e740b42f6dc5cc54a2bc37c31b0

Appendix A: Vendor Information

Below is information we have received from vendors who have patches available or upcoming for the vulnerabilities described in this advisory, as well as vendors who have confirmed that their products are not vulnerable. If your vendor's name is not in one of these lists, contact the vendor directly for information on whether their version of sendmail is vulnerable and, if so, the status of patches to address the vulnerabilities.

NOT VULNERABLE

The following vendors have reported that their products are NOT vulnerable.

Apple Computer, Inc.
Berkeley SW Design, Inc. (BSDI)
Data General Corp.
Harris
IBM
NeXT, Inc.
Pyramid
The Santa Cruz Operation (SCO) - not vulnerable, but see note below
Sun Microsystems, Inc. - Solaris 2.x (SunOS 4.x is vulnerable; see below)

In addition, we have reports that the following *products* are NOT vulnerable.

FreeBSD
NetBSD

VULNERABLE

We have reports that the following vendors' products ARE vulnerable. Patch information is provided below.

Digital Equipment Corporation

Vulnerable:	DEC OSF/1 versions 1.2, 1.3, and 2.0 DEC ULTRIX versions 4.3, 4.3A, and 4.4

Obtain and install the appropriate patch according to the instructions included with the patch. The patch that corrects the /bin/mail problem in each case is part of a comprehensive Security Enhanced Kit that addresses other problems as well. This kit has been available since May 17, 1994. It is described in DEC security advisory #0505 and in CERT bulletin VB-94:02.

1. DEC OSF/1
   Upgrade/install OSF/1 to a minimum of V2.0 and install Security Enhanced Kit CSCPAT_4061 v1.0.
2. DEC ULTRIX
   Upgrade/install ULTRIX to a minimum of V4.4 and install Security Enhanced Kit CSCPAT_4060 v1.0.

Both kits listed above are available from Digital Equipment Corporation by contacting your normal Digital support channel or by request via DSNlink for electronic transfer.

The Santa Cruz Operation (SCO)

SCO's version of /bin/mail is not vulnerable to the problems mentioned in this advisory. SCO's /bin/mail is not setuid-root. However, SCO's /bin/mail has other security-related issues that are fixed by SCO's Support Level Supplement (SLS) uod392a. To get this:

ftp:	ftp.sco.COM:/SLS/uod392a.Z	(compressed disk image)
	ftp.sco.COM:/SLS/uod392a.ltr.Z	(cover letter)
	ftp.sco.COM:/SLS/README	

Solbourne

Grumman System Support Corporation now performs all Solbourne software and hardware support. Please contact them for further information.

ftp: ftp.nts.gssc.com
phone: 1-800-447-2861
e-mail: support@nts.gssc.com

Sun Microsystems, Inc.

Current patches are listed below:

SunOS	Patch	MD5 Checksum
4.1.3	100224-13.tar.Z	90a507017a1a40c4622b3f1f00ce5d2d
4.1.3U1	101436-08.tar.Z	0e64560edc61eb4b3da81a932e8b11e1

The patches can be obtained from local Sun Answer Centers and through anonymous FTP from ftp.uu.net in the /systems/sun/sun-dist directory. In Europe, the patches are available from mcsun.eu.net in the /sun/fixes directory.

The CERT Coordination Center thanks Eric Allman, Wolfgang Ley, Karl Strickland, Wietse Venema, and Neil Woods for their contributions to mail.local.

Revision History

```
Sep. 23 1997   Updated Copyright statement

Nov. 21, 1996  Removed Appendices B & C.

               Sec. B, paragraph 3 - updated information about the

                Location of mail.local.

Aug. 30, 1996  Information previously in the README was inserted

               into the advisory, and URL formats were updated.

June 09, 1995  Appendix A - corrected patch information from Sun.
```

3 CA-1995-03: Telnet Encryption Vulnerability

Original issue date: March 3, 1995
Last revised: September 23, 1997
Updated copyright statement

A complete revision history is at the end of this file. **This advisory supersedes CA-95.03.**

The CERT Coordination Center has received reports of a serious security problem in the Berkeley Telnet clients that provide support for the experimental Telnet encryption option using the Kerberos V4 authentication. All known released versions of the BSD Telnet that support Kerberos V4 authentication and encryption are affected.

We recommend that all sites that use encrypted telnet in conjunction with Kerberos V4 obtain a patch or upgraded version of Telnet according to the instructions in Section III below.

We will update this advisory as we receive additional information. Please check advisory files regularly for updates that relate to your site.

I. Description

There is a vulnerability in Berkeley Telnet clients that support encryption and Kerberos V4 authentications. This vulnerability substantially reduces the effectiveness of the encryption.

II. Impact

Anyone who can access and read packets that make up the encrypted Telnet session can easily decrypt the session. This is possible, for example, when an intruder uses a packet sniffer on the network to intercept the Telnet sessions.

III. Solution

Obtain and install the appropriate patch according to the instructions included with the patch.

In Appendix A is a summary of the vendors who have reported to us and the status they provided, including how to obtain patches. We will update the appendix as we receive more information from vendors.

Appendix A: Vendor Information

Below is information we have received from vendors who have patches available or upcoming, along with names of vendors who have reported that their products do not have the problem.

If you have an encrypting Telnet from a vendor who is not listed, please contact that vendor for information regarding how to get a fixed version.

Vendor or Source	Status
Berkeley SW Distribution (BSD)	source-code patch available from Berkeley; also in Appendix B of this advisory
Data General Corporation	not affected by the vulnerability
Digital Equipment Corporation	not affected by the vulnerability
FTP Software, Inc.	patch available
Harris NightHawk System	not affected by the vulnerability
Hewlett-Packard Company	not affected by the vulnerability
Nat'l. Center for Supercomputer Applications (NCSA)	upgrade available
Open Software Foundation	not affected by the vulnerability
The Santa Cruz Operation, Inc.(SCO)	not affected by the vulnerability
Sequent Computer Systems	not affected by the vulnerability
Sun Microsystems, Inc.	not affected by the vulnerability

PATCH INFORMATION

Berkeley Software Distribution (BSD)

A source-code patch, along with the domestic version of the most recently released Telnet sources from Berkeley, are available by anonymous FTP from net-dist.mit.edu:/pub/telnet/telnet.patch
MD5 65d56befe3d0f1699d38de5509552578

There is also a PGP ASCII signature file for the patch in
net-dist.mit.edu:/pub/telnet/telnet.patch.sig.

This patch can also be found in CERT Advisory CA-95.03a, Appendix B. (**Note:** Do not calculate a checksum for Appendix B alone. It will not match the checksum of the FTP version of the patch because the tabs in the FTP copy have been replaced with blank spaces in the CA-95.03a Appendix B copy.)

FTP Software, Inc.

Customers of FTP Software with an encrypting telnet (provided in the PC/TCP or OnNet packages) should call the FTP technical support line at 1-800-282-4387 and ask for the "tn encrypt patch".

National Center for Supercomputer Applications (NCSA)

Users of NCSA Telnet should upgrade to the NCSA Telnet 2.6.1d7, AND install the appropriate Kerberos plug-in which are available by anonymous FTP from ftp.ncsa.uiuc.edu

Upgrade

/Mac/Telnet/Telnet2.6/prerelease/d7/Telnet2.6.1d7(68K).sit.hqx
MD5 b34b9fda59421b3b83f8df08a83f83b5

/Mac/Telnet/Telnet2.6/prerelease/d7/Telnet2.6.1d7(fat).sit.hqx
MD5 877add7c3d298111889fc3f2f272ce6f

Kerberos plug-ins

/Mac/Telnet/Telnet2.6/prerelease/AuthMan.plugin.1.0b1.hqx
MD5 df727eae184b22125f90ef1a31513fd4

/Mac/Telnet/Telnet2.6/prerelease/Kerberos_Telnet_plugin.sit.hqx
MD5 dbda691efe9038648f234397895c734d

Questions regarding NCSA Telnet should be directed to mactel@ncsa.uiuc.edu.

Appendix B: Patch for Vulnerability in Telnet Encryption Option

Index: auth.c

```
RCS file: /mit/krb5/.cvsroot/src/appl/telnet/libtelnet/auth.c,v
retrieving revision 5.5
retrieving revision 5.7
diff -u -r5.5 -r5.7
--- auth.c      1994/08/18 21:06:45     5.5
+++ auth.c      1994/11/08 04:39:02     5.7
@@ -244,7 +244,7 @@
{
register int x;
-       if (strcasecmp(type, AUTHTYPE_NAME(0))) {
+       if (!strcasecmp(type, AUTHTYPE_NAME(0))) {
                *maskp = -1;
                return(1);
        }
```

```
@@ -260,14 +260,14 @@
        int
auth_enable(type)
- -       int type;
+       char * type;
{
        return(auth_onoff(type, 1));
}
        int
auth_disable(type)
- -       int type;
+       char * type;
{
        return(auth_onoff(type, 0));
}
@@ -277,15 +277,20 @@
        char *type;
        int on;
{
- -       int mask = -1;
+       int i, mask = -1;
        Authenticator *ap;
        if (!strcasecmp(type, "?") || !strcasecmp(type, "help")) {
                 printf("auth %s 'type'\n", on ? "enable" : "disable");
                printf("Where 'type' is one of:\n");
                printf("\t%s\n", AUTHTYPE_NAME(0));
- -               for (ap = authenticators; ap->type; ap++)
+               mask = 0;
+               for (ap = authenticators; ap->type; ap++) {
+                       if ((mask & (i = typemask(ap->type))) != 0)
+                               continue;
+                       mask |= i;
                        printf("\t%s\n", AUTHTYPE_NAME(ap->type));
+               }
                return(0);
        }
@@ -293,7 +298,6 @@
                printf("%s: invalid authentication type\n", type);
                return(0);
        }
- -       mask = getauthmask(type, &mask);
        if (on)
                i_wont_support &= ~mask;
        else
@@ -317,16 +321,22 @@
auth_status()
{
        Authenticator *ap;
+       int i, mask;
        if (i_wont_support == -1)
                printf("Authentication disabled\n");
        else
                printf("Authentication enabled\n");
- -       for (ap = authenticators; ap->type; ap++)
+       mask = 0;
+       for (ap = authenticators; ap->type; ap++) {
+               if ((mask & (i = typemask(ap->type))) != 0)
+                       continue;
+               mask |= i;
                printf("%s: %s\n", AUTHTYPE_NAME(ap->type),
                        (i_wont_support & typemask(ap->type)) ?
                                        "disabled" : "enabled");
+       }
        return(1);
}
```

Index: kerberos.c

```
RCS file: /mit/krb5/.cvsroot/src/appl/telnet/libtelnet/kerberos.c,v
retrieving revision 5.5
retrieving revision 5.8
diff -u -r5.5 -r5.8
- --- kerberos.c  1994/08/18 21:07:02     5.5
+++ kerberos.c  1994/11/14 21:33:58     5.8
@@ -225,9 +225,10 @@
                register int i;
                des_key_sched(cred.session, sched);
- -               des_set_random_generator_seed(cred.session);
- -               des_new_random_key(challenge);
- -               des_ecb_encrypt(challenge, session_key, sched, 1);
+               des_init_random_number_generator(cred.session);
+               des_new_random_key(session_key);
+               des_ecb_encrypt(session_key, session_key, sched, 0);
+               des_ecb_encrypt(session_key, challenge, sched, 0);
                /*
```

```
                 * Increment the challenge by 1, and encrypt it for
                 * later comparison.
@@ -320,6 +321,11 @@
                        break;
                }
+               /*
+                * Initialize the random number generator since it's
+                * used later on by the encryption routine.
+                */
+               des_init_random_number_generator(session_key);
                des_key_sched(session_key, sched);
                memcpy((void *)datablock, (void *)data,
sizeof(Block));
                /*
@@ -337,7 +343,7 @@
                 * increment by one, re-encrypt it and send it back.
                 */
                des_ecb_encrypt(datablock, challenge, sched, 0);
- -               for (r = 7; r >= 0; r++) {
+               for (r = 7; r >= 0; r--) {
                        register int t;
                        t = (unsigned int)challenge[r] + 1;
                        challenge[r] = t;       /* ignore overflow
*/
```

Index: commands.c

```
RCS file: /mit/krb5/.cvsroot/src/appl/telnet/telnet/commands.c,v
retrieving revision 5.14
retrieving revision 5.16
diff -u -r5.14 -r5.16
```

```
- --- commands.c  1994/08/18 21:07:37     5.14

+++ commands.c  1994/11/08 06:42:49     5.16

@@ -1919,8 +1919,8 @@

};

extern int

- -       auth_enable P((int)),

- -       auth_disable P((int)),

+       auth_enable P((char *)),

+       auth_disable P((char *)),

        auth_status P((void));

static int

        auth_help P((void));

@@ -1959,6 +1959,12 @@

{

     struct authlist *c;

+    if (argc < 2) {

+      fprintf(stderr,

+          "Need an argument to 'auth' command.  'auth ?' for
help.\n");

+      return 0;

+    }

+

     c = (struct authlist *)

                genget(argv[1], (char **) AuthList, sizeof(struct
authlist));

     if (c == 0) {

@@ -2015,7 +2021,7 @@

                                                 EncryptEnable, 1, 1,
2 },
     { "disable", "Disable encryption. ('encrypt enable ?' for
more)",

                                                EncryptDisable, 0,
1, 2 },

- -    { "type", "Set encryptiong type. ('encrypt type ?' for
more)",

+    { "type", "Set encryption type. ('encrypt type ?' for more)",

                                                EncryptType, 0, 1, 1
},

     { "start", "Start encryption. ('encrypt start ?' for more)",

                                                EncryptStart, 1, 0,
1 },

@@ -2058,6 +2064,12 @@

     char *argv[];

{

     struct encryptlist *c;

+

+    if (argc < 2) {

+       fprintf(stderr,

+           "Need an argument to 'encrypt' command.  'encrypt ?' for
help.\n");

+       return 0;

+    }

     c = (struct encryptlist *)

                genget(argv[1], (char **) EncryptList, sizeof(struct
encryptlist));
```

The CERT Coordination Center wishes to thank Theodore Ts'o of the Massachusetts Institute of Technology for identifying and developing a solution to this problem. We also thank Douglas Engert of Argonne National Laboratory for pointing out the omission in our original Appendix B.

Revision History

Sep. 23. 1997 Updated copyright information

Aug. 30, 1996 Information previously in the README was inserted into the advisory.

Mar. 03, 1995 Appendix A summary list - Digital Equipment and Sequent added as "not affected by the vulnerability"

Mar. 03, 1995 This advisory superseded CA-95.03, which had a portion of the patch missing from Appendix B.

4 CA-1995-04: NCSA HTTP Daemon for UNIX Vulnerability

Original issue date: February 17, 1995
Last revised: September 23, 1997
Updated Copyright Statement

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

The CERT Coordination Center has received reports that there is a vulnerability in the NCSA HTTP Daemon V.1.3 for UNIX. Because of this vulnerability, the daemon can be tricked into executing shell commands.

If you have any questions regarding this vulnerability, please contact NCSA (Elizabeth Frank, efrank@ncsa.uiuc.edu).

We will update this advisory as we receive additional information. Please check advisory files regularly for updates that relate to your site.

I. Description

A vulnerability in the NCSA HTTP Daemon allows it to be tricked into executing shell commands.

II. Impact

Remote users may gain unauthorized access to the account (uid) under which the httpd process is running.

III. Solution

Review the text provided by NSCA (#1 below) and install the patch provided under #2 below.

1. Read the following text, which was provided by the HTTPD Team at SDG at NCSA. This text replaces Step 1 in the original version of the advisory. The NCSA text can also be found at http://hoohoo.ncsa.uiuc.edu/docs/patch_desc.html.

Beginning of Text Provided by NCSA

NCSA httpd Patch for Buffer Overflow

A vulnerability was recently discovered in the NCSA httpd. A program which will break into an HP system running the precompiled httpd has been published, along with step by step instructions. The program overflows a buffer into program space which then gets executed.

If you are running a precompiled NCSA httpd, please ftp a new copy of the binary. If you have compiled your own source code, we recommend applying the following Patch to fix the vulnerability in the NCSA HTTP Daemon V.1.3 for UNIX. It modifies the strsubfirst subroutine in util.c.

We believe that earlier versions of the server are vulnerable to a similar attack, and strsubfirst should be modified for all releases of the server. [The original version of] Cert Advisory CA-95.04 describes the problem and includes two suggested steps. We do not recommend taking step 1, which increases MAX_STRING_LEN to 8192. There are 154 occurrences of variables using MAX_STRING_LEN and changing them from 256 to 8192 bytes is going to expand the memory needed to run httpd tremendously! On top of that, httpd forks a new process (a complete copy of the parent) for each connection, which if your site gets hit a lot will use unnecessarily large amounts of memory. We have already had reports from admins who have made the change saying they are experiencing performance degradation due to swapping. Step 2, applying the patch to util.c, should be sufficient to fix the problem. There is significantly less forking in Release 1.4 of the NCSA HTTP Daemon which will be released soon.

Detecting a Break-in

If the access log contains control characters, there is a chance that someone has tried to break into your system. If your server has died recently, they failed at least one attempt. And, if your server has not crashed and there are control characters in the access log you should assume your system has been compromised.

In this case, servers which currently use the User Directive to run the server as "nobody", have limited the potential damage of an intruder to those commands which "nobody" may execute. Control Characters in the Access Log You've discovered control characters in your access log. How do you tell if was an intruder? If the beginning of the line containing the control characters begins sensibly (eg. machine name, and date (the GET periodically gets clobbered)) and ends with a series of control characters, it is a break-in attempt. If the beginning of the line starts with control characters (often nulls), this is a symptom of a collision problem that occurs when two children try to write to the access log simultaneously. This problem has only been seen with moderately to heavily loaded servers. (We are working to fix this in Release 1.4.)

Other ways to Make Your Server More Secure

A tutorial about running a secure server is available. We also recommend that the User Directive be used to run the server as "nobody".

Patched Source and Binaries

The patched source and precompiled binaries are available. We will also be correcting the source for previous releases, but we will NOT be generating binaries for previous releases.

Elizabeth Frank
efrank@ncsa.uiuc.edu

End of Text Provided by NCSA

2. Install the following patch, which performs the functionality of strsubfirst (i.e., copy src followed by dest[start] into dest) without the use of a temporary buffer.

cut here

```
*** util.c.bak  Sat May  7 21:47:15 1994
--- util.c      Thu Feb 16 04:17:07 1995
***************
*** 158,168 ****
  void strsubfirst(int start,char *dest, char *src)
  {
!     char tmp[MAX_STRING_LEN];
!     strcpy(tmp,&dest[start]);
!     strcpy(dest,src);
!     strcpy(&dest[strlen(src)],tmp);
}
/*
--- 158,174 ----
  void strsubfirst(int start,char *dest, char *src)
  {
!   int src_len, dest_len, i;
!   if ((src_len=strlen(src))<start){  /** src "fits" in dest **/
!     for (i=0;dest[i]=src[i];i++);
!     for (i=src_len;dest[i]=dest[i-src_len+start];i++);
!   }
!   else {                             /** src doesn't fit in dest
**/
!     for (dest_len=strlen(dest),i=dest_len+src_len-
start;i>=src_len;i--)
!       dest[i] = dest[i-src_len+start];
!     for (i=0;i<src_len;i++) dest[i]=src[i];
!   }
}
/*
```

---

cut here

After you apply this patch, recompile httpd, kill the current running process, and restart the new httpd.

The CERT Coordination Center thanks Steve Weeber, Carlos Varela, and Beth Frank for their support in responding to this problem.

Revision History

```
Sep. 23, 1997  Updated copyright statement
Aug. 07, 1996  Information previously in the README was inserted
               into the advisory.
Mar. 15, 1995  Sec. III - Replaced original Step 1 with text
               from NCSA.
               Updated NCSA contact information.
```

5 CA-1995-05: Sendmail Vulnerabilities

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1
====================================================================
CERT(sm) Advisory CA-95:05
Original issue date:  February 22, 1995
Last revised: September 18, 1996
              SUPERSEDED BY CA-96.20
              A complete revision history is at the end of this
file.
Topic: Sendmail Vulnerabilities
------------------------------------------------------------------
                  *** SUPERSEDED BY CA-96.20 ***
               This advisory previously superseded CA-94:12
               and all previous CERT advisories on sendmail.
```

The CERT Coordination Center has received reports of several problems with sendmail, one of which is widely known. The problems occur in many versions of sendmail (see below for details).

The CERT staff recommends installing the appropriate patches immediately. If you cannot do so, consider using one of the alternatives described in Section III.

We will update this advisory as we receive additional information. Please check advisory files regularly for updates that relate to your site.

```
------------------------------------------------------------------
I.   Description
```

There is a problem in versions of sendmail that support IDENT (RFC 1413) functionality. This problem could allow an intruder to gain unauthorized access to your system remotely (that is, without having access to an account on the system). Systems known at this time to be affected are named in the Solutions section below; see the column labeled "Remote vul?/patch status." In addition, other problems have been identified in sendmail that allow intruders to gain unauthorized privileges. Intruders need to have access to an account on your system to exploit these problems. The problems occur in many versions of sendmail. The final column of the table in the Solutions section indicates systems known at this time to be affected.

II. Impact

By exploiting the vulnerabilities, intruders may be able to read any file on the system, overwrite or destroy files, or run programs on the system. The problem in IDENT's subroutines enables intruders to exploit the vulnerability remotely. To exploit the other vulnerabilities, intruders need to have access to an account on the system.

III. Solution

A. Obtain the appropriate patch from your vendor and install it according to the instructions included with the patch. Below is a summary of information we have received from vendors. More details, including how to obtain patches, are in the Appendix A of this advisory. If your vendor's name is not on this list, please contact your vendor directly.

Vendor or Source	Remote vul?/patch status (IDENT)	Local vul?/patch status
Eric Allman		
version 8.6.10	no/ --	no/ --
all other versions	yes/upgrade avail.	yes/upgrade avail.
Apple Computer, Inc.		
v.3.1.1, 3.1	no/ --	yes/patch avail.
earlier versions	yes/see appendix	yes/see appendix
Berkeley Software Design, Inc. (BSDI)		
version 2.0	no/ --	yes/patch avail. soon
other versions	yes/patch avail. soon	yes/patch avail. soon
Cray Computer Corporation (Craycos)	no/ --	yes/patch avail.
Data General Corporation	no/ --	no/ --
Digital Equipment Corp.	no/ --	yes/patch avail.
Harris Comp.Systems Corp.	yes/patch avail.	yes/patch avail.
Hewlett-Packard Company	no/ --	yes/patch avail.by Feb 23
IBM Corporation	no/ --	yes/patch avail.
IDA	See Appendix A.	pls. update to latest sendmail
Motorola	yes/patch avail.	yes/patch avail.
Open Software Foundation	no/ --	yes/see appendix
The Santa Cruz Operation	no/ --	yes/patch avail. soon
Sequent Computer Systems	no/ --	yes/patch avail.
Silicon Graphics (SGI)	no/ --	yes/patch avail.
Solbourne (Grumman)	no/ --	yes/patch avail.
Sony Corporation	yes/patch avail.	yes/patch avail.
Sun Microsystems, Inc.	no/ --	yes/patch avail.

B. Install sendmail 8.6.10, which is freely available (see Appendix A for locations). This version fixes all the problems described in this advisory. Be aware that, depending upon the currently installed sendmail program, switching to a different sendmail may require significant effort (such as rewriting the sendmail.cf file.)
C. Until you are able to install the appropriate patch or sendmail 8.6.10, we recommend the following workarounds.

1. To protect against remote attacks only:
If you are running sendmail versions 8.6.6 through 8.6.9, you can turn off the IDENT protocol by adding the following line to the configuration file and then restarting sendmail:

```
Orident=0
```

If you have difficulty doing so, consult your documentation or vendor for guidance.

If you are running 8.6.5 or earlier you cannot disable IDENT in this way. Instead, you should upgrade to version 8.6.10.

2. To provide limited protection against local attacks:
Install the "sendmail wrapper" that is provided in Appendix B of this advisory. The wrapper is also available by anonymous FTP from

```
info.cert.org:/pub/tools/sendmail/sendmail_wrapper/sendmail_wrapper.c
MD5 = 5c930d9d139dfaa1dfc9de6c40ddf8c6

ftp.auscert.org.au:/pub/auscert/tools/sendmail_wrapper.c
MD5 = 5c930d9d139dfaa1dfc9de6c40ddf8c6

ftp.cert.dfn.de:/pub/tools/net/sendmail-wrapper/sendmail-wrapper.c
MD5 = 5c930d9d139dfaa1dfc9de6c40ddf8c6
```

3. To restrict sendmail's program mailer facility, obtain and install the sendmail restricted shell program (smrsh) by Eric Allman (the original author of sendmail), following the directions included with the program. This program may be obtained via anonymous FTP from

```
             ftp://info.cert.org/pub/tools/smrsh
             ftp://ftp.uu.net/pub/security/smrsh
             The checksums are
             MD5 (README)  = fc4cf266288511099e44b664806a5594
             MD5 (smrsh.8) = 35aeefba9714f251a3610c7b1714e355
             MD5 (smrsh.c) = d4822ce7c273fc8b93c68e39ec67739c
```

....

Appendix A: Vendor Information

Below is information we have received from vendors who have patches available or upcoming for the vulnerabilities described in this advisory.

Eric Allman
Sendmail version 8.6.10 is not vulnerable. This version is available by anonymous FTP from

ftp.cs.berkeley.edu:/ucb/sendmail
ftp.uu.net:/networking/mail/sendmail/UCB
info.cert.org:/pub/tools/sendmail/sendmail.8.6.10
ftp.cert.dfn.de:/pub/tools/net/sendmail
ftp.auscert.org.au:/pub/coast/mirrors/ftp.cs.berkeley.edu/ucb/sendmail

In all of the above locations, the MD5 checksums are the same,
MD5 (sendmail.8.6.10.base.tar.Z) = 4ab8ac267b1eaf8d1725c14cf4b2e885
MD5 (sendmail.8.6.10.cf.tar.Z) = c70c576697bbbf047ed379a7b98633f6
MD5 (sendmail.8.6.10.misc.tar.Z) = 6212390ca0bb4b353e29521f1aab492f
MD5 (sendmail.8.6.10.patch) = 08d6f977c171ea858f1e940163212c3a
MD5 (sendmail.8.6.10.xdoc.tar.Z) = 8b2252943f365f303b6302b71ef9a841

Apple Computer, Inc.
An upgrade to A/UX version 3.1 (and 3.1.1) for these vulnerabilities is available. The upgrade is a replacement of the sendmail binary. It is available via anonymous FTP from ftp.support.apple.com: pub/apple_sw_updates/US/Unix/A_UX/supported/3.x/sendmail/.

The compressed binary has the following signature:
MD5 (sendmail.Z) = 31bb15604517630f46d7444a6cfab3f1

Uncompress(1) this file and replace the existing version in /usr/lib; be sure to preserve the hard links to /usr/ucb/newaliases and /usr/ucb/mailq, kill the running sendmail and restart.

Earlier versions of A/UX are not supported by this patch. Users of previous versions are encouraged to update their system or compile the latest version of sendmail available from ftp.cs.berkeley.edu. Customers should contact their reseller for any additional information.

Berkeley Software Design. Inc. (BSDI)
BSD/OS V2.0 is vulnerable to the local user problems, but not the remote user (IDENT) problem.

All earlier releases of BSD/OS are vulnerable to both problems. Patches are being developed and will be made available via anonymous FTP on ftp.bsdi.com in the directory "bsdi/support".

BSDI Contact Information:

BSDI Customer Support
Berkeley Software Design, Inc.
7759 Delmonico Drive
Colorado Springs, CO 80919
Toll Free: +1 800 ITS BSD8 (+1 800 486 2738)
Phone: +1 719 260 8114
Fax: +1 719 598 4238
Email: support@bsdi.com

Cray Computer Corporation (Craycos)

A new version of sendmail, one that does not have the problem, is available from CCC. Please contact your site analyst for more information. You may also contact CCC Field Support using the address below. e-mail: support@craycos.com

----

Digital Equipment Corporation

Digital Equipment Corporation strongly urges Customers to upgrade to the latest versions of ULTRIX V4.4 or DIGITAL DEC OSF/1 V3.2, then apply the appropriate sendmail solution kit. (For more information, please refer to article SSRT0320-1486.) Digital has corrected this potential vulnerability and provided kits containing new binaries. The appropriate kits and images are identified as follows:

ULTRIX	DEC OSF/1
ULTSENDMAIL_E01044	OSFSENDMAIL_E01032

The above kits were available (FLASH notice via DSNlink) as of June 1, 1995, and can be obtained through your normal Digital support channels.

Please refer to the applicable Release Note information prior to upgrading your installation. NOTE: For non-contract/non-warranty customers there may be a nominal charge for the kit, to cover the costs of media and handling.

Harris Computer Systems Corporation

Request the appropriate patch for Harris NightHawk Systems, as follows:

System	Patch
cx/ux 7.1	cx7.1-030
cx/ux 6.2	cx6.2-114
cx/sx 6.2	cx6.2-114

If you need further information, contact the Harris Support Hotline 1-800-245-6453.

Hewlett-Packard Company

```
Hewlett-Packard HP-UX           Patches available by 2/23/95
                                Vulnerable to:   -d DEBUG option
                                            Latest queue problem
                                Not Vulnerable to: IDENT problem
```

```
Apply patch PHNE_5264 (series 700/800, HP-UX 9.x), or
            PHNE_5263 (series 700/800, HP-UX 8.x), or
            PHNE_5260 (series 300/400, HP-UX 9.0), or
            PHNE_5259 (series 300/400, HP-UX 8.x)
```

You can get patches via:

1. Ftp / email / kermit to HP SupportLine

To obtain a copy of the HP SupportLine email service user's guide, send the following in the TEXT PORTION OF THE MESSAGE to support@support.mayfield.hp.com (no Subject is required): send guide

2. World Wide Web: http://support.mayfield.hp.com

If you need further information, contact

HP SupportLine: 1-415-691-3888
phone: 1-415-691-3680
telnet/ftp: support.mayfield.hp.com (192.6.148.19)

IBM Corporation

A possible security exposure exists in the bos.obj sendmail subsystem in all AIX releases. The user can cause arbitrary data to be written into the sendmail queue file.
Non-privileged users can affect the delivery of mail, as well as run programs as other users.

Workaround

A. Apply the patch for this problem. The patch is available from software.watson.ibm.com. The files will be located in the /pub/aix/sendmail in compressed tar format. The MD5 checksum for the binary file is listed below, ordinary "sum" checksums follow as well.

File	sum	MD5 Checksum
sendmail.tar.Z	35990	e172fac410a1b31f3a8c0188f5fd3edb

B. The official fix for this problem can be ordered as Authorized Program Analysis Report (APAR) IX49257

To order an APAR from IBM in the U.S. call 1-800-237-5511 and ask for shipment as soon as it is available (in approximately two weeks). APARs may be obtained outside the U.S. by contacting a local IBM representative.

IDA

IDA sendmail is no longer being supported and it is recommended that users update to the latest sendmail.

```
--------------------
Motorola Computer Group (MCG)
```

The following MCG platforms are vulnerable:

```
        R40
        R32 running CNEP add-on product
        R3 running CNEP add-on product
```

The following MCG platforms are not vulnerable:

```
        R32     not including CNEP add-on product
        R3      not including CNEP add-on product
        R2
        VMEEXEC
        VERSADOS
```

The patch is available and is identified as "patch_43004 p001" or "SCML#5552". It is applicable to OS revisions from R40V3 to R40V4.3.

For availability of patches for other versions of the product contact your regional MCG office at the numbers listed below.

Obtain and install the appropriate patch according to the instructions included with the patch.

The patch can be obtained through anonymous ftp from ftp.mcd.mot.com [144.191.210.3] in the pub/patches/r4 directory. The patch can also be obtained via sales and support channels. Questions regarding the patch should be forwarded to sales or support channels.
For verification of the patch file:

```
        Results of      sum -r  == 27479 661
                        sum     == 32917 661
                        md5     == 8210c9ef9441da4c9a81c527b44defa6
```

Contact numbers for Sales and Support for MCG:

```
                United States (Tempe, Arizona)
                Tel:    +1-800-624-0077
                Fax:    +1-602-438-3865
        Europe (Brussels, Belgium)
                Tel:    +32-2-718-5411
                Fax:    +32-2-718-5566
        Asia Pacific / Japan (Hong Kong)
                Tel:    +852-966-3210
                Fax:    +852-966-3202
        Latin America / Australia / New Zealand (U.S.)
                Tel:   +1 602-438-5633
                Fax:   +1 602-438-3592
```

Open Software Foundation

The local vulnerability described in the advisory can be exploited in OSF's OSF/1 R1.3 (this is different from DEC's OSF/1). Customers should apply the relevant portions of cert's fix to their source base. For more information please contact OSF's support organization at osf1-defect@osf.org.

The Santa Cruz Operation

SCO systems are not vulnerable to the IDENT problem.
Systems running the MMDF mail system are not vulnerable to the remote or local problems.

The following releases of SCO products are vulnerable to the local problems.

==

SCO TCP/IP 1.1.x for SCO Unix System V/386 Operating System Release 3.2

Versions 1.0 and 2.0

SCO TCP/IP 1.2.x for SCO Unix System V/386 Operating System Release 3.2 Versions 4.x

SCO TCP/IP 1.2.0 for SCO Xenix System V/386 Operating System Release 2.3.4

SCO Open Desktop Lite Release 3.0

SCO Open Desktop Release 1.x, 2.0, and 3.0

SCO Open Server Network System, Release 3.0

SCO Open Server Enterprise System, Release 3.0

Patches are currently being developed for the release 3.0 and 1.2.1 based products. The latest sendmail available from SCO, on Support Level Supplement (SLS) net382d, is also vulnerable.

Contacts for further information:
e-mail: support@sco.COM
USA, Canada, Pacific Rim, Asia, Latin America
6am-5pm Pacific Daylight Time (PDT)

1-408-425-4726 (voice)
1-408-427-5443 (fax)
Europe, Middle East, Africa: 9am-5:30pm British Standard Time (BST)

+44 (0)923 816344 (voice)
+44 (0)923 817781 (fax)

Sequent Computer Systems

Sequent customers should contact Sequent Customer Service and request the Fastpatch for sendmail.

phone: 1-800-854-9969.
e-mail: service-question@sequent.com

Silicon Graphics, Inc.

At the time of writing of this document, patches/binaries are planned for IRIX versions 4.x, 5.2, 5.3, 6.0, and 6.0.1 and will be available to all SGI customers.

The patches/binaries may be obtained via anonymous ftp (ftp.sgi.com) or from your support/service provider.

On the anonymous ftp server, the binaries/patches can be found in either ~ftp/patches or ~ftp/security directories along with more current pertinent information.

For any issues regarding this patch, please, contact your support/service provider or send email to cse-security-alert@csd.sgi.com.

Sony Corporation
NEWS-OS 6.0.3   vulnerable; Patch SONYP6022 [sendmail] is available.
NEWS-OS 6.1   vulnerable; Patch SONYP6101 [sendmail] is available.
NEWS-OS 4.2.1   vulnerable; Patch 0101 [sendmail-3] is available.

Note that this patch is not included in 4.2.1a+.

Patches are available via anonymous FTP in the /pub/patch/news-os/un-official directory on ftp1.sony.co.jp [202.24.32.18]:

4.2.1a+/0101.doc	describes about patch 0101 [sendmail-3]
4.2.1a+/0101_C.pch	patch for NEWS-OS 4.2.1C/a+C
4.2.1a+/0101_R.pch	patch for NEWS-OS 4.2.1R/RN/RD/aRD/aRS/a+R
6.0.3/SONYP6022.doc	describes about patch SONYP6022 [sendmail]
6.0.3/SONYP6022.pch	patch for NEWS-OS 6.0.3
6.1/SONYP6101.doc	describes about patch SONYP6101 [sendmail]
6.1/SONYP6101.pch	patch for NEWS-OS 6.1

Filename	BSD Checksum	SVR4 Checksum
4.2.1a+/0101.doc	55361 2	19699 4
4.2.1a+/0101_C.pch	60185 307	25993 614
4.2.1a+/0101_R.pch	35612 502	31139 1004
6.0.3/SONYP6022.doc	03698 2	36652 4
6.0.3/SONYP6022.pch	41319 436	20298 871
6.1/SONYP6101.doc	40725 2	3257 3
6.1/SONYP6101.pch	37762 434	4624 868

MD5 checksums are:
MD5 (4.2.1a+/0101.doc) = c696c28abb65fffa5f2cb447d4253902
MD5 (4.2.1a+/0101_C.pch) = 20c2d4939cd6ad6db0901d6e6d5ee832
MD5 (4.2.1a+/0101_R.pch) = 840c20f909cf7a9ac188b9696d690b92
MD5 (6.0.3/SONYP6022.doc) = b5b61aa85684c19e3104dd3c4f88c5c5
MD5 (6.0.3/SONYP6022.pch) = 1e4d577f380ef509fd5241d97a6bcbea
MD5 (6.1/SONYP6101.doc) = 62601c61aef99535acb325cf443b1b25
MD5 (6.1/SONYP6101.pch) = 87c0d58f82b6c6f7811750251bace98c
If you need further information, contact your vendor.

Solbourne

Grumman System Support Corporation now performs all Solbourne software and hardware support. Please contact them for further information.

e-mail: support@nts.gssc.com
phone: 1-800-447-2861

The Solbourne sendmail security patch, equivalent to Sun patch 100377-19, has been released and is available via anonymous ftp from ftp.nts.gssc.com.

The 4.1C patch is in /pub/support/OS4.1C/P95031405.tar.Z,
and the 4.1B patch is in /pub/support/OS4.1B/P95031501.tar.Z.

There are also index and md5.checksums files in these directories.

MD5 (P95031405.tar.Z) = 28cede699837d4bf78bc24a212feb705
MD5 (P95031501.tar.Z) = eb6df9ece991681f4c3d2801297cabd3

This patch closes the vulnerabilities described in CERT advisory CA-95:05.

Sun Microsystems, Inc.

Sun has developed patches for all supported platforms and architectures, including Trusted Solaris, Solaris x86, and Interactive Unix. Note that Sun no longer supports the sun3 architecture and versions of the operating system that precede 4.1.3.

Patches are available for the versions of SunOS shown below.

OS version	Patch ID	Patch File Name
4.1.3	100377-19	100377-19.tar.Z
4.1.3_U1	101665-04	101665-04.tar.Z
4.1.4	102356-01	102356-01.tar.Z
5.3	101739-07	101739-07.tar.Z
5.4	102066-04	102066-04.tar.Z
5.4_x86	102064-04	102064-04.tar.Z

Patches have also been created for Sun's Trusted Solaris and Interactive Unix products. To obtain either, contact your Sun representative.

BSD and SVR4 checksums and MD5 digital signatures for the compressed tar archives:

File Name	BSD Checksum	SVR4 Checksum	MD5 Digital Signature
100377-19.tar.Z	01093	212 22539	423 8CE1C1E04B8A640F2B90EAE1AA813351
101665-04.tar.Z	28743	213 48403	426 EA5E76D0B1A43756E58AEA18AB6D7BCC
101739-07.tar.Z	30088	214 60567	428 CF85226BAF145D6B1BD457E189E771BE
102064-04.tar.Z	33127	188 30212	375 276F05037CA1A72D1D2019A98C241327
102066-04.tar.Z	13253	214 47552	428 AE190B5CAD8E0CFA8DE7DD059E4A7E71
102356-01.tar.Z	53116	203 58382	406 B23AC4EFDC8D82B6528E46E27717EBD8

The checksums shown above are from the BSD-based checksum (on 4.1.x, /bin/sum; on Solaris 2.x, /usr/ucb/sum) and from the SVR4 version on Solaris 2.x (/usr/bin/sum).

Patches can be obtained from local Sun Answer Centers and through anonymous FTP from ftp.uu.net in the /systems/sun/sun-dist directory. In Europe, the patches are available from mcsun.eu.net in the /sun/fixes directory.

The patches are available via World Wide Web at http://sunsolve1.sun.com.

....

Appendix B: Sendmail Wrapper

This wrapper can be used to improve security until you can install a vendor patch or sendmail version 8.6.10. Note that it does not address all known sendmail vulnerabilities.

```
/*
**  sendmail_wrapper.c - wrap sendmail to prevent newlines in command line
**                       and clean up the environment.
**
**  Authors:    Eric Halil, Danny Smith
**              AUSCERT
**              c/o Prentice Centre
**              The University of Queensland
**              Qld.  4072.
**              Australia
**              22-Feb-1995
**
**  Disclaimer:  The use of this program is at your own risk.  It is
**               designed to combat a particular vulnerability, and may
**               not combat other vulnerabilities, either past or future.
**               The decision to use this program is yours, as are the
**               consequences of its use.
**
**               This program is designed to be an interim relief measure
**               until appropriate patches can be obtained from your vendor.
**
**  Installation instructions
**  =========================
**
**  1.  su to root.
**
**  2.  Determine the location of sendmail.  On SunOS and Ultrix
**      systems, it is located in the /usr/lib directory.  On BSDI
**      systems, it is located in the /usr/sbin directory.  For example
**      purposes only, /usr/lib will be used in the following instructions
**      steps.
**
**  3.  Copy the sendmail program to sendmail.real.  Change the permissions
**      on the copy of sendmail.
**
**              # cd /usr/lib
**              # cp sendmail sendmail.real
**              # chmod 0700 sendmail.real
**
**  4.  Determine the permissions, owner, and group of sendmail.  This
**      information will be used later.
**
**      For BSD users:
**              # ls -lg sendmail
**      For System V users:
**              # ls -l sendmail
**
**  5.  Edit this wrapper program and define REAL_SENDMAIL.  By default,
**      REAL_SENDMAIL is defined as "/usr/lib/sendmail.real".
**
**  6.  Compile this program in a directory other than /usr/lib.  For
**      example to use /tmp, first copy this file into /tmp.
**
**              # cd /tmp
**              # cc -O -o sendmail sendmail_wrapper.c
**
**  7.  Copy this new wrapper program into the directory containing sendmail.
**      Make sure this directory and its parent directories are protected so
**      only root is able to make changes to files in the directory.  This
**      will replace the existing sendmail.  The following steps should be
**      executed quickly.
**
**      Users will not be able to send e-mail during the time when the
**      wrapper is copied into place until the chmod command has been
**      executed.  Use the information from step #4 and set the permissions
**      owner, and group of the new sendmail.
**
**              # cp sendmail /usr/lib/sendmail
**              # cd /usr/lib
**              # chown root sendmail
**              # chmod 4511 sendmail
**
**  8.  Kill the running sendmail process and start the new sendmail.
**
**      For SunOS and Ultrix:
**              # kill -9 `head -1 /etc/sendmail.pid`
**              # /usr/lib/sendmail -bd -q1h
**
```

```
**      For BSDI:
**              # kill -9 `head -1 /var/run/sendmail.pid`
**              # /usr/sbin/sendmail -bd -q1h
**
**      For other systems, follow your vendors guidelines or use the
**      following command.  Kill the processes and start the new sendmail.
**              # ps -auxw | grep sendmail | grep -v grep
**              # kill -9 (process id numbers)
**              # ./sendmail -bd -q1h
**
**  9.  Test that mail still works.
** Version 1.1  22-Feb-1995.
*/
#include <stdio.h>
/*
**      REAL_SENDMAIL needs to be defined using the full pathname
**      of the real sendmail.  A few known locations have been defined.
*/
#ifdef sun
#define REAL_SENDMAIL   "/usr/lib/sendmail.real"
#endif
#ifdef ultrix
#define REAL_SENDMAIL   "/usr/lib/sendmail.real"
#endif
#if defined (__bsdi__) || defined(__386BSD__) || defined(__FreeBSD__) || defined(__NetBSD__)
#define REAL_SENDMAIL   "/usr/sbin/sendmail.real"
#endif
int main( argc, argv, envp)
int     argc;
char    *argv[];
char    *envp[];
{
    char        *cp;
    int         i;
    int         j;
    int         status;
/*
**  Ensure that there are no newlines in the arguments
*/
    for ( i = 1; i < argc; i++)
    {
        for ( cp = argv[ i]; *cp != '\0'; cp++)
        {
            if ( ( *cp == '\r') || ( *cp == '\n'))
            {
                *cp = ' ';
            }
        }
    }
```

```
/*
**  While we are at it, let's clean up the environment
**  Remove LD_*, IFS, and PATH environment variables before execing
*/
    i = 0;
    while( envp[ i] != NULL)
    {
        if ( strncmp( envp[ i], "LD_", 3) == 0)
        {
            j = i;
            while ( envp[ j] != NULL)
            {
                envp[ j] = envp[ j + 1];
                j++;
            }
            continue;
        }
        if ( strncmp( envp[ i], "IFS=", 4) == 0)
        {
            j = i;
            while ( envp[ j] != NULL)
            {
                envp[ j] = envp[ j + 1];
                j++;
            }
            continue;
        }
        if ( strncmp( envp[ i], "PATH=", 5) == 0)
        {
            j = i;
            while ( envp[ j] != NULL)
            {
                envp[ j] = envp[ j + 1];
                j++;
            }
            continue;
        }
/*
**  Now check for newlines in environment variables
*/
        for ( cp = envp[ i]; *cp != '\0'; cp++)
        {
            if ( ( *cp == '\r') || ( *cp == '\n'))
            {
                *cp = ' ';
            }
        }
/*
**  next environment variable
*/
```

```
        i++;
    }
/*
** exec the real sendmail now
*/
    status = execve( REAL_SENDMAIL, argv, envp);
    perror( "execve sendmail");
    return( status);
}
```

The CERT Coordination Center thanks Eric Allman, Wolfgang Ley, Danny Smith, and Eric Halil for their support in responding to this problem.

If you believe that your system has been compromised, contact the CERT Coordination Center or your representative in the Forum of Incident Response and Security Teams (FIRST).

If you wish to send sensitive incident or vulnerability information to CERT staff by electronic mail, we strongly advise that the e-mail be encrypted. The CERT Coordination Center can support a shared DES key, PGP (public key available via anonymous FTP on info.cert.org), or PEM (contact CERT staff for details).

Internet E-mail: cert@cert.org
Telephone: +1 412-268-7090 (24-hour hotline)

CERT personnel answer 8:30 a.m.-5:00 p.m. EST(GMT-5)/EDT(GMT-4), and are on call for emergencies during other hours.

Fax: +1 412-268-6989

Postal address: CERT Coordination Center

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890
USA

CERT advisories and bulletins are posted on the USENET newsgroup comp.security.announce. If you would like to have future advisories and bulletins mailed to you or to a mail exploder at your site, please send mail to cert-advisory-request@cert.org.

Past advisories, CERT bulletins, information about FIRST representatives, and other information related to computer security are available for anonymous FTP from info.cert.org.

CERT is a service mark of Carnegie Mellon University.

Revision history

```
Sep. 18, 1996  Superseded by CA-96.20.
Aug. 30, 1996  Information previously in the README was inserted
               into the advisory.
Oct. 18, 1995  Appendix A - Digital Equipment, added date that
                the patch kits were available.
Sep. 18, 1995  Appendix A - added or updated information for Digital
               Equipment, IDA, Solbourne (Grumman), and Sun.
Sep. 18, 1995  Sec. III.C.3 - added Step 3: install smrsh.
```

```
-----BEGIN PGP SIGNATURE-----
Version: PGP for Personal Privacy 5.0
Charset: noconv
iQA/AwUBOBS+Flr9kb5qlZHQEQLH7ACeNfbQhAJHkF1DWW3fTSmQgVl8M3MAn3jR
/bjuPxjKcy45torQQkYpafiU
=09FS
-----END PGP SIGNATURE-----
```

6 CA-1995-06: Security Administrator Tool for Analyzing Networks (SATAN)

Original issue date: April 3, 1995
Last revised: September 23, 1997
Updated Copyright statement

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

The CERT Coordination Center staff examined beta version 0.51 of the Security Administrator Tool for Analyzing Networks (SATAN). This advisory initially contained information based on our review of this pre-release version. When the official release became available, we updated the advisory based on version 1.1.1.

1. What is SATAN?

SATAN is a testing and reporting tool that collects a variety of information about networked hosts. The currently available documentation can be found at ftp://ftp.win.tue.nl/pub/security/satan_doc.tar.Z.

SATAN gathers information about specified hosts and networks by examining network services (for example, finger, NFS, NIS, ftp, and rexd). It can then report this data in a summary format or, with a simple rule-based system, investigate potential security problems. Problems are described briefly and pointers provided to patches or workarounds. In addition to reporting vulnerabilities, SATAN gathers general network information (network topology, network services run, types of hardware and software being used on the network). As described in the SATAN documentation, SATAN has an exploratory mode that allows it to probe hosts that have not been explicitly specified. Thus, SATAN could probe not only targeted hosts, but also hosts outside your administrative domain.

Section 4 below lists the vulnerabilities currently probed by SATAN.

After the release of SATAN 1.0, we published a separate advisory describing a vulnerability in SATAN. If you do not already have a copy of CA-95.07a, we strongly urge you to obtain a copy from www.cert.org/advisories/CA-95.07a.REVISED.satan.vul.html.

As we receive new information about SATAN, we will update advisories CA-95.06 (SATAN in general) and CA-95.07a (vulnerability in SATAN). We encourage you to check our advisories regularly for updates to relating to your site.

2. Potential Impact of SATAN

SATAN was designed as a security tool for system and network administrators. However, given its wide distribution, ease of use, and ability to scan remote networks, SATAN is also likely to be used to locate vulnerable hosts for malicious reasons. It is also possible that sites running SATAN for a legitimate purpose will accidentally scan your system via SATAN's exploratory mode.

Although the vulnerabilities SATAN identifies are not new, the ability to locate them with a widely available, easy-to-use tool increases the level of threat to sites that have not taken steps to address those vulnerabilities. In addition, SATAN is easily extensible. After it is released, modified versions might scan for other vulnerabilities as well and might include code to compromise systems.

3. How to Prepare for the Release of SATAN

- Examine your systems for the vulnerabilities described below and implement security fixes accordingly.
- In addition to reading the advisories cited for specific vulnerabilities below, consult the following documents for guidance on improving the security of your systems:

- ftp://ftp.cert.org/pub/tech_tips/intruder_detection_checklist
  ftp://ftp.cert.org/pub/tech_tips/UNIX_configuration_guidelines
  ftp://ftp.cert.org/pub/tech_tips/anonymous_ftp_config
  ftp://ftp.cert.org/pub/tech_tips/packet_filtering
- Contact your vendor for information on available security patches, and ensure that all patches have been installed at your site.

- Use the tools listed in Section 5 to assist you in assessing and improving the security of your systems.

4. Vulnerabilities Probed by SATAN

Listed below are vulnerabilities that beta version 0.51 of SATAN tests for, along with references to CERT advisories and other documents where applicable.

Administrators should verify the state of their systems and perform corrective actions as necessary. We cannot stress enough the importance of good network configuration and the need to install all available patches.

1. NFS export to unprivileged programs
2. NFS export via portmapper
3. Unrestricted NFS export

See CERT advisory CA-94.15 for security measures you can take to address NFS vulnerabilities.

The following advisories also address problems related to NFS:

CA-94.02.REVISED.SunOS.rpc.mountd.vulnerability
CA-93.15.SunOS.and.Solaris.vulnerabilities
CA-92.15.Multiple.SunOS.vulnerabilities.patched
CA-91.21.SunOS.NFS.Jumbo.and.fsirand

4. NIS password file access
   See CERT advisory CA-92.13 for information about SunOS 4.x machines using NIS, and CA-93.01 for information about HP machines.
5. rexd access
   We recommend filtering the rexd service at your firewall and commenting out rexd in the file /etc/inetd.conf.

   See CERT advisory CA-92.05 for more information about IBM AIX machines using rexd, and CA-91.06 for information about NeXT.
6. Sendmail vulnerabilities
   See CERT advisory CA-95.05 for the latest information we have published about sendmail.
7. TFTP file access
   See CERT advisory CA-91.18 for security measures that address TFTP access problems. In addition, CA-91.19 contains information for IBM AIX users.
8. Remote shell access
   We recommend that you comment out rshd in the file /etc/inetd.conf or protect it with a TCP wrapper. A TCP/IP wrapper program is available from
   ftp://ftp.cert.org/pub/tools/tcp_wrappers/
9. Unrestricted X server access
   We recommend filtering X at your firewall. Additional advice about packet filtering is available by anonymous FTP from
   ftp://ftp.cert.org/pub/tech_tips/packet_filtering
10. Writable FTP home directory
    See CERT advisory CA-93.10.
    Guidance on anonymous FTP configuration is also available from
    ftp://ftp.cert.org/pub/tech_tips/anonymous_ftp_config
11. wu-ftpd vulnerability
    See CA-93.06 and CA-94.07 for more information about ftpd.
12. Unrestricted dial-out modem available via TCP.
    Place modems behind a firewall or put password or other extra authentication on them (such as S/Key or one-time passwords). For information on one-time passwords, see CERT advisory CA-94.01, Appendix B.

Note: In addition to our FTP archive at ftp.cert.org, CERT documents are available from the following sites, and others which you can locate by using archie:

ftp://coast.cs.purdue.edu/pub/mirrors/cert.org/cert_advisories
ftp://unix.hensa.ac.uk/pub/uunet/doc/security/cert_advisories
ftp://ftp.luth.se/pub/misc/cert/cert_advisories
ftp://ftp.switch.ch/network/security/cert_advisories
ftp://corton.inria.fr/CERT/cert_advisories
ftp://ftp.inria.fr/network/cert_advisories
ftp://nic.nordu.net/networking/security/cert_advisories

5. Currently Available Tools

The following tools are freely available now and can help you improve your site's security before SATAN is released.

COPS and ISS can be used to check for vulnerabilities and configuration weaknesses.

COPS is available from ftp//ftp.cert.org:/pub/tools/cops/*

ISS is available from ftp://ftp.uu.net/usenet/comp.sources.misc/volume39/iss
CERT advisory CA-93.14 contains information about ISS.

TCP wrappers can provide access control and flexible logging to most network services. These features can help you prevent and detect network attacks. This software is available by anonymous FTP from ftp://ftp.cert.org/pub/tools/tcp_wrappers/*.

The TAMU security package includes tools to check for vulnerabilities and system configuration weaknesses, and it provides logging and filtering of network services. This software is available by anonymous FTP from ftp://net.tamu.edu/pub/security/TAMU/*.

The Swatch log file monitor allows you to identify patterns in log file entries and associate them with actions. This tool is available from ftp://ee.stanford.edu/pub/sources/swatch.tar.Z.

6. Detecting Probes

One indication of attacks by SATAN, and other tools, is evidence of a heavy scan of a range of ports and services in a relatively short time. Many UNIX network daemons do not provide sufficient logging to determine if SATAN is probing the system. TCP wrappers, the TAMU tools, and Swatch can provide the logging you need.

New tools are becoming available on the network to help you detect probes, but the CERT staff has not evaluated them.

Although detection tools can be helpful, keep in mind that their effectiveness depends on the nature and availability of your logs and that the tools may become less effective as SATAN is modified. The most important thing you can do is take preventive action to secure your systems.

7. Using SATAN

Running SATAN on your systems will provide you with the same information an attacker would obtain, allowing you to correct vulnerabilities. If you choose to run SATAN, we urge you to read the documentation carefully. Also, note the following:

- It is easy to accidentally probe systems you did not intend to. If this occurs, the probed site may view the probe(s) as an attack on their system(s).
- Take special care in setting up your configuration file, and in selecting the probe level when you run SATAN.
- Explicitly bound the scope of your probes when you run SATAN. Under "SATAN Configuration Management," explicitly limit probes to specific hosts and exclude specific hosts.
- When you run SATAN, ensure that other users do not have read access to your SATAN directory.
- In some cases, SATAN points to CERT advisories. If the link does not work for you, try getting the advisories by anonymous FTP.
- Install all relevant security patches for the system on which you will run SATAN.
- Ensure that the SATAN directory tree cannot be read by users other than root.
- Execute SATAN only from the console of the system on which it is installed (e.g., do not run SATAN from an X terminal, from a diskless workstation, or from a remote host).
- Ensure that the SATAN directory tree is not NFS-mounted from a remote system.
- It is best to run SATAN from a system that does not support multiple users.

8. Getting more information about SATAN

The SATAN authors report that SATAN 1.1.1 is available from many sites, including:

ftp://ftp.win.tue.nl/pub/security/satan-1.1.1.tar.Z
ftp://ftp.win.tue.nl/pub/security/satan-1.1.1.README
ftp://ftp.win.tue.nl/pub/security/satan_doc.tar.Z
ftp://ftp.win.tue.nl/pub/security/satan_doc.README

To get a current list of sites, send mail to majordomo@wzv.win.tue.nl and put in the body of your message

```
get satan mirror-sites
```

You can also use archie to locate sites that have SATAN.

MD5 checksums for SATAN:

satan-1.1.1.README = 3f935e595ab85ee28b327237f1d55287
satan-1.1.1.tar.Z = de2d3d38196ba6638b5d7f37ca8c54d7
satan-1.1.1.tar.Z.asc = a9261070885560ec11e6cc1fe0622243
satan_doc.README = 4ebe05abc3268493cdea0da786bc9589
satan_doc.tar.Z = 951d8bfca033eeb483a004a4f801f99a
satan_doc.tar.Z.asc = 3216053386f72347956f2f91d6c1cb7c

Also available is "Improving the Security of Your Site by Breaking Into It" (admin-guide-to-cracking.101), a 1993 paper in which the authors give their rationale for creating SATAN.

The CERT Coordination Center staff thanks Dan Farmer and Wieste Venema for the the opportunity to examine pre-release versions of SATAN. We also appreciate the interaction with the response teams at AUSCERT, CIAC, and DFN-CERT, and feedback from Eric Allman.

UPDATES

Note to users of LINUX SATAN: There was a posting to USENET that a Trojan horse was introduced into a version of LINUX SATAN binaries archived on ftp.epinet.com. CERT staff have not verified that this Trojan horse exists; however, if you are using LINUX SATAN and believe your version may be compromised, we suggest you obtain additional information from ftp://ftp.epinet.com/pub/linux/security.

Revision History

Sep. 23, 1997 Updated copyright statement

Aug. 30, 1996 Information previously in the README was inserted into the advisory. Updated tech tip references.

Apr. 11, 1995 Updated information based on SATAN 1.1.1 (original advisory was based on beta version 0.51):

Introduction - added reference to CA-95.07a

Sec. 4 - added information on SATAN probe for unrestricted modems

Sec. 6 - added a note on tools for detecting probes

Sec. 7 - added five additional precautions

Sec. 8 - where to get a copy of SATAN checksums for SATAN and documentation where to send comments about SATAN

Apr. 11, 1995 Sec. 3 - pathnames corrected in Sec. 3

Sec. 4-5 - colons noted in (and subsequently removed from) URLs

Apr. 11, 1995 Updates section - added a note on LINUX SATAN

7 CA-1995-07: Vulnerability in SATAN

Original issue date: April 21, 1995
Last revised: September 23, 1997
Update copyright statement

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

This is a revised CERT advisory.
It addresses inaccurate information in CA-95.07
and contains information about SATAN 1.1.1.
Supersedes CA-95.07

There was a potential vulnerability introduced into systems running SATAN 1.0 and earlier, as described below. The problem has been addressed in version 1.1 and later. The CERT/CC team recommends that you take the precautions described in Section III below before you run SATAN and that you upgrade to the latest version of SATAN--currently 1.1.1.

The following two statements from CA-95.07 are inaccurate.

1. This statement is incorrect: "Note that SATAN 1.1 is expected to check systems for this SATAN 1.0 vulnerability as part of scanning other systems."
2. This statement is misleading: "This vulnerability affects all systems that support the use of SATAN with the HTML interface." For SATAN 1.0 and earlier, whether a system is vulnerable depends on the system configuration, the net browser supporting SATAN, and how SATAN is used. The problem has been solved in later versions of SATAN.

We will update this advisory as we receive additional information. Please check advisory files regularly for updates that relate to your site.

For an overview of a beta version of SATAN, see CERT advisory CA-95.06.

I. Description

In SATAN version 1.0, access to the SATAN processes is protected by a session key (also referred to as a "magic cookie" or "password"). SATAN itself never sends this session key over the network. However, depending on the configuration at your site, the supporting HTML browser, and how you use SATAN, your session key may be disclosed through the network. Local or remote users who obtain your session key can run perl scripts that are on the system running SATAN.

If you use SATAN only through the command line interface, your system is not vulnerable to the problem because there is no session key.

Additional details are in the "SATAN Password Disclosure" tutorial provided with SATAN. We have included the tutorial as an Appendix B of this advisory.

II. Impact

If the session key is disclosed while SATAN 1.0 is running, unauthorized local or remote users can execute perl scripts as the user of the process running SATAN (typically root).

III. Solution

1. Obtain and install SATAN version 1.1.1, which addresses the problem.

For details on how the problem is addressed, see the section entitled "Additional SATAN Defenses" in the SATAN Password Disclosure tutorial. The SATAN authors also provide guidance on protecting access; see the tutorial section, "Preventing SATAN Password Disclosure." SATAN 1.1.1 is available from many sites, including

ftp://ftp.win.tue.nl/pub/security/satan-1.1.1.tar.Z
ftp://ftp.win.tue.nl/pub/security/satan-1.1.1.README
ftp://ftp.win.tue.nl/pub/security/satan-1.1.1.tar.Z.asc

MD5 (satan-1.1.1.tar.Z) = de2d3d38196ba6638b5d7f37ca8c54d7
MD5 (satan-1.1.1.README) = 3f935e595ab85ee28b327237f1d55287
MD5 (satan-1.1.1.tar.Z.asc) = a9261070885560ec11e6cc1fe0622243

To locate other sites, you can send mail to majordomo@wzv.win.tue.nl and put in the body of the message (not the subject line):

get satan mirror-sites

There are reports of modified copies of SATAN, so ensure that the copy that you obtain is authentic by checking the MD5 checksum or SATAN author Wietse Venema's PGP signature. Appendix A of this advisory contains his PGP key.

We urge you to read the SATAN documentation carefully before running SATAN.

2. We also recommend that you take the following precautions:

- Install all relevant security patches for the system on which you will run SATAN.
- Execute SATAN only from the console of the system on which it is installed (e.g., do not run SATAN from an X terminal, from a diskless workstation, or from a remote host).
- Ensure that the SATAN directory tree is not NFS-mounted (or AFS, etc.) from a remote system.
- Ensure that the SATAN directory tree cannot be read by users other than root.
- Do not open any URLs outside your own system and site while running the browser started by SATAN. For example, do not use previously stored URLs such as those found in bookmarks and pull-down menus.
- Do not link to any URLs outside your own system and site while running the browser started by SATAN. If you use external links while SATAN is running from the SATAN browser, se-

curity can be compromised on the system from which you are executing SATAN. So, for example, do not use previously stored links such as those found in bookmarks and pull-down menus.

Appendix A: Wietse Venema's PGP Key

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6
mQCNAirDhV8AAAED/i4LrhQ/mwOgam8ZfQpEcxYoE9kru5oRDGtoVeKae/4bUver
aGX7qVtskD6vwPwr2FF6JW2c+z2oY4JGPGUArORiigoT82/q6vqT0Wm1jIPsXQSB
ZCkBoyvBcmXEi+J7eDBbWLPDxeDimgrORbAIQ4uikRafs8KlpNyA8qbVMny5AAUR
tCV3aWV0c2UgdmVuZW1hIDx3aWV0c2VAd3p2Lndpbi50dWUubmw+
=PQUu

-----END PGP PUBLIC KEY BLOCK-----
```

Appendix B: Tutorial - SATAN Password Disclosure

The following tutorial can be found in satan-1.1.1/html/tutorials/vulnerability/SATAN_password_disclosure.html.

SATAN Password Disclosure

SUMMARY

SATAN password disclosure via flawed HTML clients or environmental problems

IMPACT

Unauthorized users may execute commands through SATAN

BACKGROUND

By default, SATAN runs as a custom HTML (hypertext markup language) server, executing requests from a user-provided HTML browser, or client program. Examples of common HTML clients are Netscape, NCSA Mosaic and Lynx.

An HTML client request is nothing but a network message, and network messages may be sent by any user on the network. To defend itself against requests from unauthorized users, SATAN takes the following precautions:

- SATAN generates a session key, to be used as a secret password, each time it starts up an HTML client. The session key is in the form of a 32-byte quasi-random number. The number is called quasi-random because it is impossible to generate real random numbers using only software.
- SATAN creates HTML files with the secret password embedded in URL (uniform resource locator) links. The HTML file access permissions are restricted to the owner of the SATAN process (and the superuser).

- SATAN rejects HTML requests whose URL does not contain the current SATAN password. This requirement prevents access by unauthorized clients, provided that the current SATAN password is kept secret.

The protection scheme used by SATAN is in essence the same as the scheme used by many implementations of the X Window system: MIT magic cookies. These secrets are normally kept in the user's home directory, in a file called .Xauthority. Before it is granted access to the screen, keyboard and mouse, an X client program needs to prove that it is authorized, by handing over the correct magic cookie. This requirement prevents unauthorized access, provided that the magic cookie information is kept secret.

THE PROBLEM

It is important that the current SATAN password is kept secret. When the password leaks out, unauthorized users can send commands to the SATAN HTML server where the commands will be executed with the privileges of the SATAN process.

Note that SATAN generates a new password every time you start it up under an HTML client, so if you are suspicious, simply restart the program.

SATAN never sends its current password over the network. However, the password, or parts of it, may be disclosed due to flaws in HTML clients or due to weak protection of the environment that SATAN is running in. One possible scenario for disclosure is:

- When the user selects other HTML servers from within a SATAN session, some HTML client programs (Netscape and Lynx) disclose the current SATAN URL, including SATAN password information. The intention of this feature is to help service providers find out the structure of the world-wide web. However, the feature can also reveal confidential information. With version 1.1 and later, SATAN displays a warning when the HTML client program exhibits this questionable (i.e. stupid) feature.

Other scenarios for SATAN password disclosure are discussed in the next section, as part of a list of counter measures.

PREVENTING SATAN PASSWORD DISCLOSURE

The security of SATAN is highly dependent on the security of environment that it runs in. In the case of an X Window environment:

- Avoid using the xhost mechanism, but use xauth and MIT magic cookies or better. Otherwise, unauthorized users can see and manipulate everything that happens with the screen, keyboard and mouse. Of course, this can also be a problem when you are not running the SATAN program at all.

Steps that can help to keep the X magic cookie information secret:

- Avoid sharing your home directory, including .Xauthority file, with other hosts. Otherwise, X magic cookie information may be captured from the network while the X software accesses that file, so that unauthorized users can take over the screen, keyboard and mouse.

- Avoid running X applications with output to a remote display. Otherwise, X magic cookie information can be captured from the network while X clients connect to the remote display, so that unauthorized users can take over the screen, keyboard and mouse.

Finally, steps that can help to keep the current SATAN password secret:

- Avoid sharing the SATAN directories with other hosts. Otherwise, SATAN password information may be captured from the network while the HTML software accesses passworded files, so that unauthorized users can take over the SATAN HTML server.
- Avoid running SATAN with output to a remote display. Otherwise, SATAN password information can be captured from the network while URL information is shown on the remote display, so that unauthorized users can take over the SATAN HTML server.

ADDITIONAL SATAN DEFENSES

The SATAN software spends a lot of effort to protect your computer and data against password disclosure. With version 1.1 and later, SATAN even attempts to protect you after the password has fallen into the hands of unauthorized users:

- SATAN displays a warning and advises the user to not contact other HTML servers from within a SATAN session, when it finds that the HTML client program reveals SATAN password information as part of parent URL information.
- SATAN rejects requests that appear to come from hosts other than the one it is running on, that refer to resources outside its own HTML tree, or that contain unexpected data.
- SATAN terminates with a warning when it finds a valid SATAN password in an illegal request: SATAN assumes the password has fallen into the hands of unauthorized users and assumes the worst.

The CERT Coordination Center staff thanks Wietse Venema for his cooperation and assistance with this revised advisory.

Revision History

```
Sep. 23, 1997 - Updated copyright statement

Aug. 30, 1996 - Information previously in the CA-95.07 and CA-95.07a
README files was inserted into the advisory.
```

8 CA-1995-08: Sendmail v.5 Vulnerability

Original issue date: August 17, 1995
Last revised: September 23, 1997
Updated copyright statement

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

The CERT Coordination Center has received reports of a vulnerability in sendmail version 5. Although this version is several years old, it is still in use. The vulnerability enables intruders to gain unauthorized privileges, including root. We recommend installing all patches from your vendor or moving to the current version of Eric Allman's sendmail (version 8.6.12).

The vulnerability is currently present in all versions of IDA sendmail and in some vendors' releases of sendmail. The vendors who have reported to us are listed in Section I.

We will update this advisory as we receive additional information. Please check advisory files regularly for updates that relate to your site.

I. Description

In sendmail version 5, there is a vulnerability that intruders can exploit to create files, append to existing files, or execute programs.

The vulnerability is currently present in all versions of IDA sendmail and in some vendors' releases of sendmail.

Many vendors have previously installed upgrades or developed patches to address the problem; some are working on patches now. Here is a summary of vendors who reported to us as of the date of this advisory.

More details can be found in the appendix of this advisory, which we will update as we receive additional information.

If you do not see your vendor's name or if you have questions about the version of sendmail at your site, please contact your vendor directly.

Source or Vendor

Eric Allman
Apple Computer, Inc.
Berkeley SW. Design
Cray Research, Inc.
Data General Corp.
Digital Equipment Corp.
Harris Computer Systems

Hewlett-Packard Company
IBM Corporation
NEC Corporation
NeXT Computer, Inc.
Open Software Foundation
The Santa Cruz Operation
Silicon Graphics Inc.
Solbourne (Grumman)
Sun Microsystems, Inc.

Freely available and distributable software:

Users of the freely available operating systems Linux (systems using sendmail rather than smail), NetBSD, and FreeBSD should upgrade to sendmail 8.6.12.

II. Impact

Local and remote users can create files, append to existing files or run programs on the system. Exploitation can lead to root access.

III. Solution

A. What to do

IDA users:

Convert to sendmail 8.6.12.

Other users:

Check the vendor information in the appendix of this advisory.

Ensure that you have kept current with upgrades and patches from your vendor.

If no patch is currently available, an alternative is to install sendmail 8.6.12.

B. What you need to know about sendmail

1. **Location**

   Sendmail is available by anonymous FTP from

   ftp://ftp.cs.berkeley.edu/ucb/sendmail
   ftp://ftp.cert.org/pub/tools/sendmail/sendmail.8.6.12
   ftp://ftp.auscert.org.au/pub/mirrors/ftp.cs.berkeley.edu/ucb/sendmail
   ftp://ftp.cert.dfn.de/pub/tools/net/sendmail/

The checksums are

MD5 (sendmail.8.6.12.base.tar.Z) = 31591dfb0dacbe0a7e06147747a6ccea
MD5 (sendmail.8.6.12.cf.tar.Z) = c60becd7628fad715df8f7e13dcf3cc6
MD5 (sendmail.8.6.12.misc.tar.Z) = 6212390ca0bb4b353e29521f1aab492f
MD5 (sendmail.8.6.12.patch) = 10961687c087ef30920b13185eef41e8
MD5 (sendmail.8.6.12.xdoc.tar.Z) = 8b2252943f365f303b6302b71ef9a841

2. **Additional Security**

To restrict sendmail's program mailer facility, obtain and install the sendmail restricted shell program (smrsh) by Eric Allman (the original author of sendmail), following the directions included with the program.

You should run smrsh with any UNIX system that is running sendmail, regardless of vendor or version. Even with Eric Allman's sendmail version 8.6.12, it is necessary for security-conscious sites to use the smrsh program, as this carries out preprocessing of mail headers and adds an extra layer of defense by controlling what programs can be spawned by the incoming mail message. Note that smrsh has now been included as part of the sendmail distribution (effective with 8.7).

We also urge you to ensure that all patches are installed for the distribution of sendmail you are using. Regardless of the vendor or version of your UNIX systems and sendmail, the general advice to "run the smrsh tool in conjunction with the most recently patched version of sendmail for your system" holds true.

Copies of smrsh may be obtained via anonymous FTP from

ftp://ftp.cert.org/pub/tools/smrsh
ftp://ftp.uu.net/pub/security/smrsh

Checksum information:

BSD Sum
30114 5 README
25757 2 smrsh.8
46786 5 smrsh.c

System V Sum
56478 10 README
42281 4 smrsh.8
65517 9 smrsh.c

MD5 Checksum
MD5 (README) = fc4cf266288511099e44b664806a5594
MD5 (smrsh.8) = 35aeefba9714f251a3610c7b1714e355
MD5 (smrsh.c) = d4822ce7c273fc8b93c68e39ec67739c

3. **Notes on installation**

   Depending upon the currently installed sendmail program, switching to a different sendmail may require significant effort (such as rewriting the sendmail.cf file.)

Appendix: Vendor Information

Below is information we have received from vendors about the vulnerability in sendmail version 5. If you do not see your vendor's name below, contact the vendor directly for information.

Eric Allman

Sendmail 8.6.10 and later are not vulnerable. The current version is 8.6.12. Because the current version addresses vulnerabilities that appear in earlier versions, it is a good idea to use 8.6.12.

Sendmail is available by anonymous FTP from

ftp://ftp.cs.berkeley.edu/ucb/sendmail
ftp://ftp.cert.org/pub/tools/sendmail/sendmail.8.6.12
ftp://ftp.auscert.org.au/pub/mirrors/ftp.cs.berkeley.edu/ucb/sendmail
ftp://ftp.cert.dfn.de/pub/tools/net/sendmail/

The checksums are

MD5 (sendmail.8.6.12.base.tar.Z) = 31591dfb0dacbe0a7e06147747a6ccea
MD5 (sendmail.8.6.12.cf.tar.Z) = c60becd7628fad715df8f7e13dcf3cc6
MD5 (sendmail.8.6.12.misc.tar.Z) = 6212390ca0bb4b353e29521f1aab492f
MD5 (sendmail.8.6.12.patch) = 10961687c087ef30920b13185eef41e8
MD5 (sendmail.8.6.12.xdoc.tar.Z) = 8b2252943f365f303b6302b71ef9a841

Apple Computer, Inc.

[The following information also appeared in CERT advisory CA-95.05, "Sendmail Vulnerabilities."]

An upgrade to A/UX version 3.1 (and 3.1.1) for these vulnerabilities is available. The upgrade replaces the sendmail binary with the 8.6.10 version. It is available via anonymous FTP from ftp.support.apple:

pub/apple_sw_updates/US/Unix/A_UX/supported/3.x/sendmail/

It is also available via anonymous FTP from abs.apple.com:

pub/abs/aws95/patches/sendmail/

In both cases the compressed binary has the following signature:

MD5 (sendmail.Z) = 31bb15604517630f46d7444a6cfab3f1

Uncompress(1) this file and replace the existing version in /usr/lib; be sure to preserve the hard links to /usr/ucb/newaliases and /usr/ucb/mailq, kill the running sendmail and restart.

Earlier versions of A/UX are not supported by this patch. Users of previous versions are encouraged to update their system or compile the latest version of sendmail available from ftp.cs.berkeley.edu.

Customers should contact their reseller for any additional information.

Berkeley Software Design, Inc. (BSDI)

BSD/OS V2.0.1 is not vulnerable.

BSD/OS V2.0 users should install patch U200-011, available from ftp.bsdi.com in bsdi/patches/U200-011.

BSDI Support contact information:
Phone: +1 719 536 9346
EMail: support@bsdi.com

Cray Research, Inc.

not vulnerable

Data General Corporation

DG/UX 5.4R3.00 and 5.4R3.10 (and associated Trusted version) are vulnerable. Patches in progress now.

The upcoming release (R4.10 and R4.11) will not have this vulnerability since these releases ship sendmail version 8.

Digital Equipment Corp.

A patch for SENDMAIL (ULTSENDMAIL_EO1044 & OSFSENDMAIL_E01032) has been available for some time, so if you have kept current with patches you are not vulnerable to this particular reported problem.

If you have not applied the kits above, Digital Equipment Corporation strongly urges customers to upgrade to the latest versions of ULTRIX V4.4 or DIGITAL DEC OSF/1 V3.2, then apply the appropriate sendmail solution kit.

The above kits can be obtained through your normal Digital support channels or by access (kit) request via DSNlink, DSIN, or DIA.

Grumman Systems Support Corporation (GSSC)

GSSC now performs all Solbourne software and hardware support.

We recommend running sendmail 8.6.10 (or later revision.) 8.6.12 has proven reliable in production use on Solbourne systems.

We plan to release the Solbourne version of the Sun patch when it becomes available.

Contact info:

```
ftp: ftp.nts.gssc.com
phone: 1-800-447-2861
email: support@nts.gssc.com
```

Harris Computer Systems

not vulnerable

Hewlett-Packard Company

Hewlett-Packard issued security bulletin #25 on April 2, 1995 announcing patches and describing a fix. The patches are

```
PHNE_5402 (series 700/800, HP-UX 9.x), or

PHNE_5401 (series 700/800, HP-UX 8.x), or

PHNE_5384 (series 300/400, HP-UX 9.x), or

PHNE_5383 (series 300/400, HP-UX 8.x), or

PHNE_5387 (series 700, HP-UX 9.09), or

PHNE_5388 (series 700, HP-UX 9.09+), or

PHNE_5389 (series 800, HP-UX 9.08)
```

The bulletin is available from the HP SupportLine and from http://www.hp.com
in the HPSL category and from http://support.mayfield.hp.com.

Patches may be obtained from HP via FTP (this is NOT anonymous FTP) or the HP SupportLine. To obtain HP security patches, you must first register with the HP SupportLine. The registration instructions are available via anonymous FTP at ftp.cert.org in the file "pub/vendors/hp/supportline_and_patch_retrieval".

HP SupportLine: 1-415-691-3888
phone: 1-415-691-3680
telnet/ftp: support.mayfield.hp.com
WWW: http://www.hp.com
http://support.mayfield.hp.com.

IBM Corporation

A patch (ptf U425863) has been available for AIX 3.2 for some time. To determine if you have this ptf on your system, run the following command:

```
% lslpp -lB U425863
```

If you have not already applied the patch, you can order it from IBM as APAR ix40304 To order APARs from IBM in the U.S., call 1-800-237-5511. To obtain APARs outside of the U.S., contact your local IBM representative.

NEC Corporation

OS	Version	Status
EWS-UX/V(Rel4.0)	R1.x - R6.x	vulnerable
EWS-UX/V(Rel4.2)	R7.x - R10.x	vulnerable patch available
EWS-UX/V(Rel4.2MP)	R10.x	vulnerable patch available
UP-UX/V	R1.x - R4.x	vulnerable
UP-UX/V(Rel4.2MP)	R5.x - R7.2	vulnerable patch available except for R5.x
UX/4800	R11.x	not vulnerable

Contacts for further information: email: UXcert-CT@d2.bsd.nes.nec.co.jp.

NeXT Computer, Inc.

The sendmail executables included with all versions of NEXTSTEP up to and including release 3.3 are vulnerable to this problem. The SendmailPatch previously released for NEXTSTEP 3.1 and 3.2 is also vulnerable.

An updated patch is planned which will address this vulnerability. The availability of this patch will be indicated in the NeXTanswers section of http://www.next.com/. For further information you may contact NeXT's Technical Support Hotline at (+1-800-955-NeXT) or via email to ask_next@NeXT.com.

Open Software Foundation

not vulnerable

The Santa Cruz Operation

Support Level Supplement (SLS) net382e, contains a patched version of sendmail for the following releases:

SCO TCP/IP Runtime System Release 1.2.1
SCO Open Desktop Lite Release 3.0
SCO Open Desktop Release 3.0
SCO Open Server Network System Release 3.0
SCO Open Server Enterprise System Release 3.0

SCO OpenServer 5 contains Sendmail version 8.6.8, and contains fixes to all problems reported in this and previous sendmail advisories. Users of previous releases should consider updating.

NOTE: The MMDF (M)ulti-Channel (M)emorandum (D)istribution (F)acility is the default mail system on SCO systems. The MMDF mail system is not affected by any of the problems mentioned in these advisories. Administrators who wish to use sendmail must specifically configure the system to do so during or after installation.

To acquire SLS net382e:

```
Anonymous ftp on the Internet:

==============================

ftp://ftp.sco.COM/SLS/net382e.Z         (disk image)

ftp://ftp.sco.COM/SLS/net382e.ltr.Z     (documentation)

Anonymous uucp:

===============

United States:

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

sosco!/usr/spool/uucppublic/SLS/net382e.Z (disk image)

sosco!/usr/spool/uucppublic/SLS/net382e.ltr.Z (documentation)

United Kingdom:

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

scolon!/usr/spool/uucppublic/SLS/net382e.Z (disk image)

scolon!/usr/spool/uucppublic/SLS/net382e.ltr.Z (documentation)
```

The telephone numbers and login names for the machines sosco and scolon

are provided with the default /usr/lib/uucp/Systems file shipped with

every SCO system.

The checksums for the files listed above are as follows:

```
file                 sum -r                    md5

===========================     ================================

net382e.Z:      29715  1813     41efeaaa855e4716ed70c12018014092

net382e.ltr.Z   52213    14     287ba6131519cba351bc58cb32880fda
```

The Support Level Supplement is also available on floppy media from SCO Support at the following telephone numbers:

```
         USA/Canada: 6am-5pm Pacific Daylight Time (PDT)

         -----------

         1-408-425-4726  (voice)

         1-408-427-5443  (fax)

         Pacific Rim, Asia, and Latin American customers: 6am-5pm Pacific

        ------------------------------------------------ Daylight Time

                                                          (PDT)

         1-408-425-4726  (voice)

         1-408-427-5443  (fax)

         Europe, Middle East, Africa: 9am-5:00pm Greenwich Mean Time (GMT)

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

         +44 1923 816344 (voice)

         +44 1923 817781 (fax)
```

For further information, contact SCO at one of the above numbers, send electronic mail to support@sco.COM , or see the SCO Web Page at: http://www.sco.COM.

Silicon Graphics Inc.

On February 22, 1995, Silicon Graphics issued security advisory 19950201 addressing sendmail issues being raised at the time and previous older version sendmail issues. Patches are still available and as part of these patches, sendmail version 8.6.12 is provided as standard. At the time of this writing here is the patch information.

**** IRIX 3.x ****
Unfortunately, Silicon Graphics Inc, no longer supports the IRIX 3.x operating system and therefore has no patches or binaries to provide.

However, two possible actions still remain: 1) upgrade the system to a supported version of IRIX (see below) and then install the binary/patch or 2) obtain the sendmail source code from anonymous FTP at ftp.cs.berkeley.edu and compile the program manually.

**** IRIX 4.x ****
For the IRIX operating system version 4.x, a manually installable binary replacement has been generated and made available via anonymous ftp and/or your service/support provider. The binary is sendmail.new.Z and is installable on all 4.x platforms.

Binaries can be found at ftp://ftp.sgi.com/ftp/Patches/4.x but not at the alternative location, ~ftp/Security.

```
##### Checksums as of August 17, 1995, 5 p.m. EDT ####

Filename:                 sendmail.new.Z

Algorithm #1 (sum -r):    30749 422 sendmail.new.Z

Algorithm #2 (sum):       62511 422 sendmail.new.Z

MD5 checksum:             AB327D85D40085D74E9C230EB1A002C3
```

Note: SGI plans to upgrade the IRIX 4.x patch soon. If there is a difference between the checksums of the file you obtain and those reported here, you should rely on SGI's <sendmail-filename>.pgp.and.chksums file.

After obtaining the binary, it may be installed with the instructions below:

```
          1) Become the root user on the system.

                % /bin/su -

                Password:

                #

        2) Stop the current mail processes.

                # /etc/init.d/mail stop

        3) Rename the current sendmail binary to a temporary
```

```
   name.

        # mv /usr/lib/sendmail /usr/lib/sendmail.stock

4) Change permissions on the old sendmail binary so it can not

   be used anymore.

        # chmod 0400 /usr/lib/sendmail.stock

5) Uncompress the binary.

        # uncompress /tmp/sendmail.new.Z

6) Put the new sendmail binary into place (in the example
   here the binary was retrieved via anonymous ftp and put
   in /tmp)

        # mv /tmp/sendmail.new /usr/lib/sendmail

7) Insure the correct permissions and ownership on the new
   sendmail.

        # chown root.sys /usr/lib/sendmail

        # chmod 4755 /usr/lib/sendmail

8) Restart the mail system with the new sendmail binary in place.

        # /etc/init.d/mail start

9) Return to normal user level.

        # exit
```

**** IRIX 5.0.x, 5.1.x ****
For the IRIX operating systems versions 5.0.x, 5.1.x, an upgrade to 5.2 or better is required first. When the upgrade is completed, then the patch described in the next section "**** IRIX 5.2, 5.3, 6.0, 6.0.1 ***" can be applied.

**** IRIX 5.2, 5.3, 6.0, 6.0.1 ****
For the IRIX operating system versions 5.2, 5.3, 6.0 and 6.0.1, an inst-able patch has been generated and made available via anonymous ftp and/or your service/support provider. The patch is number 332 and will install on IRIX 5.2, 5.3, 6.0 and 6.0.1 .

The SGI anonymous ftp site is ftp.sgi.com (192.48.153.1). Patch 332 can be found in the following directories on the ftp server:

~ftp/Security
or

~ftp/Patches/5.2
~ftp/Patches/5.3
~ftp/Patches/6.0
~ftp/Patches/6.0.1

For obtaining security information, patches or assistance, please contact your SGI support provider.

If there are questions about this patch information, email can be sent to cse-security-alert@csd.sgi.com.

For reporting new SGI security issues, email can be sent to security-alert@sgi.com.

Solbourne

see Grumman Systems Support Corporation

Sun Microsystems, Inc.

Solaris 2.x is not vulnerable.

Sun OS 4.1.3, 4.1.37_u1, and 4.1.4 are vulnerable, and a patch will be available soon.

This patch can be obtained from local Sun Answer Centers and through anonymous FTP from ftp.uu.net in the /systems/sun/sun-dist directory. In Europe, the patch is available from mcsun.eu.net (192.16.202.1) in the /sun/fixes directory.

The CERT Coordination Center staff thanks the vendors listed in this advisory, along with Karl Strickland and Neil Woods for their support in the development of this advisory.

Revision History

```
Sep. 23, 1997  Updated copyright statement

Aug. 07, 1996  Information previously in the README was inserted
into the advisory.

Nov. 07, 1995  Sec. III.B.2 - emphasized that smrsh should be run
with all versions of sendmail.

Sep. 20, 1995  Sec. I - changed "public domain" to "freely available."

Appendix -  added an entry for Data General.
```

```
Aug. 21, 1995  Sec. III.B and appendix, Eric Allman - added a German
FTP site for sendmail and corrected the URL for Australia.

Appendix, Silicon Graphics - corrected information for 4.x

Appendix, Sun - corrected a typo in the OS number
```

9 CA-1995-09: Solaris ps Vulnerability

Original issue date: August 29, 1995
Last revised: September 23, 1997
Updated Copyright statement

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

The text of this advisory is taken primarily from AUSCERT advisory AA-95.07, with their permission.

A vulnerability exists in Solaris systems that allows a race condition to be exploited to gain root access. The essential problem is that the *ps(1)* program maintains a data file in the /tmp directory, and the /tmp directory is world-writable, allowing users to delete other users' files in /tmp. This vulnerability affects Solaris 2.x (SunOS 5.x) systems.

An exploit program for this vulnerability has been published. We urge you to take the actions described in Section III as soon as possible.

We will update this advisory as we receive additional information. Please check advisory files regularly for updates that relate to your site.

I. Description

A race condition exists in at least one Solaris 2.x (SunOS 5.x) system program that can be exploited to gain root access if the user has access to the temporary files. Access to temporary files may be obtained if the permissions on the /tmp and /var/tmp directories are set incorrectly. The permissions on the /tmp directory are often reset incorrectly by the system if tmpfs (which is mounting swap as /tmp) is in use.

II. Impact

Users logged in to the system may gain unauthorized root privileges.

III. Solution

A. Determine if your system is vulnerable

To determine if you are running tmpfs, the following command can be used to verify if the file system for /tmp is swap:

```
% /usr/sbin/df -k /tmp

Filesystem          kbytes    used   avail capacity  Mounted on

swap                 28348     12    28336     0%    /tmp
```

or look in the file /etc/vfstab for the configuration line:

```
#device     device   mount    FS      fsck    mount     mount

#to mount   to fsck  point    type    pass    at boot   options

swap          -      /tmp     tmpfs     -      yes         -
```

If either of these two conditions exist, then you are running tmpfs and the system may automatically reset the permission bits of /tmp at the next reboot.

To verify if your configuration is currently vulnerable, the following command may be used:

```
% /usr/bin/ls -ld /tmp

drwxrwxrwt   2 root     root       61 Aug 15 12:12 /tmp
```

If the sticky bit (t) is not set (it will be an x), then the system is vulnerable. In addition, we recommend that the owner and group for /tmp be changed to root and root, respectively.

B. Perform the following workarounds

These workarounds have been verified with Sun Microsystems. Apply these workarounds until you an install a patch. (Patch information is in Sec. C. below.)

1. Immediate - fix /tmp permissions

A workaround that takes effect immediately is to set the sticky bit on the /tmp directory using the following command as root:

```
# /usr/bin/chmod 1777 /tmp
```

Note that this command must be performed after each reboot if you are mounting swap as /tmp (using tmpfs).

In addition, the ownership and group membership of the /tmp directory should be verified using /usr/bin/ls -ld /tmp, and if incorrect may be reset by:

```
# /usr/bin/chown root /tmp

# /usr/bin/chgrp root /tmp
```

The AUSCERT UNIX Security Checklist addresses this issue in Section 5.5. This section is reproduced in the appendix of this advisory. The entire AUSCERT checklist may be obtained from these locations.

Sites outside of Australia should use the ftp.cert.org FTP site.

ftp://ftp.cert.org/pub/tech_tips/AUSCERT_checklist_1.1
ftp://ftp.auscert.org.au/pub/auscert/papers/unix_security_checklist_1.1

2. Permanent - make the above change to /tmp permissions permanent

The change noted in item B.1 above will be lost upon reboot. To make the changes permanent, create the following script as /etc/init.d/tmpfsfix:

```
-----------------------------cut here--8<---------------------------

#!/bin/sh

if [ -d /tmp ]

then

   /usr/bin/chmod 1777 /tmp

   /usr/bin/chgrp root /tmp

   /usr/bin/chown root /tmp

fi

------------------------------cut here---8<-------------------------
```

After creating this file, the following commands should be issued as root to make the file executable, set appropriate owner and group, and create the necessary symbolic link to ensure that it is executed upon reboot appropriately:

```
   # /usr/bin/ln -s /etc/init.d/tmpfsfix /etc/rc2.d/S06tmpfix

   # /usr/bin/chmod 744  /etc/init.d/tmpfsfix

   # /usr/bin/chown root /etc/init.d/tmpfsfix

   # /usr/bin/chgrp sys /etc/init.d/tmpfsfix

   # /bin/rm -f /etc/rc3.d/S79tmpfix
```

If you have done item B.1 above, you can reboot at your leisure. Otherwise, reboot your system now. In either case, verify the permissions of /tmp immediately after your next system reboot.

3. Check /var/tmp permissions

We recommend that you also check and correct the /var/tmp directory. Note that this directory is not usually mounted as tmpfs, so it normally would not be subject to automatic resetting of its permission bits on reboot.

```
% /usr/bin/ls -ld /var/tmp

drwxrwxrwt   2 root     root      512 Aug 15 11:35 /var/tmp
```

C. Install a vendor patch

On September 20, 1995, Sun Microsystems, Inc., provided the following information in their advisory.

Begin Text provided by vendor

II. Announcement of patches for Solaris 2.x "ps_data" vulnerability

A. Patch list

We have produced patches for the versions of SunOS shown below.

OS version	Patch ID	Patch File Name
5.3	101545-02	101545-02.tar.Z
5.4	102711-01	102711-01.tar.Z
5.4_x86	102712-01	102712-01.tar.Z

B. Patch notes

1. SunOS 4.1.x systems are not affected by this bug. 2. The fix has been applied to the upcoming version of Solaris.

III. Checksum Table

In the checksum table we show the BSD and SVR4 checksums and MD5 digital signatures for the compressed tar archives.

File Name	BSD Checksum	SVR4 Checksum			MD5 Digital Signature
101545-02.tar.Z	41218	77	47754	153	A8FB866780E7207D26CF16210BCFDC83
102711-01.tar.Z	17256	69	20376	138	98A449372C5ABBDB7C37B08BFE0E6ED7
102712-01.tar.Z	29867	68	56717	136	E324004BB8C09990B2790CB5D29D3AF5

The checksums shown above are from the BSD-based checksum (on 4.1.x, /bin/sum; on Solaris 2.x, /usr/ucb/sum) and from the SVR4 version on Solaris 2.x (/usr/bin/sum).

End Text provided by vendor

Appendix: Excerpt from AUSCERT UNIX Security Checklist (Version 1.1) 5.5 File Permissions

- ENSURE that the permissions of /etc/utmp are set to 644.
- ENSURE that the permissions of /etc/sm and /etc/sm.bak are set to 2755.
- ENSURE that the permissions of /etc/state are set to 644.
- ENSURE that the permissions of /etc/motd and /etc/mtab are set to 644.
- ENSURE that the permissions of /etc/syslog.pid are set to 644.
  [**NOTE:** this may be reset each time you restart syslog.]
- DO consider removing read access to files that users do not need to access.
- ENSURE that the kernel (e.g., /vmunix) is owned by root, has group set to 0 (wheel on SunOS) and permissions set to 644.
- ENSURE that /etc, /usr/etc, /bin, /usr/bin, /sbin, /usr/sbin, /tmp and /var/tmp are owned by root and that the sticky-bit is set on /tmp and on /var/tmp (see G.14). Refer to the AUSCERT Advisory AA-95:05 (see A.1).
- ENSURE that there are no unexpected world writable files or directories on your system.
  See G.15 for example commands to find group and world writable files and directories.
- CHECK that files which have the SUID or SGID bit enabled, should have it enabled (see G.16).
- ENSURE the umask value for each user is set to something sensible like 027 or 077. (Refer to section E.1 for a shell script to check this).
- ENSURE all files in /dev are special files.

  Special files are identified with a letter in the first position of the permissions bits. See G.17 for a command to find files in /dev which are not special files or directories.
  Note: Some systems have directories and a shell script in /dev which may be legitimate. Please check the manual pages for more information.

- ENSURE that there are no unexpected special files outside /dev. See G.18 for a command to find any block special or character special files.

The CERT Coordination Center staff thanks AUSCERT, the Australian response team, for their permission to reuse text from their advisory AA-95.07 and for their cooperation and assistance.

UPDATES

If anyone has trouble retrieving the electronic file CA-95.09.Solaris.ps.vul, they should use the file name CA-95.09.Solaris-ps.vul.

Revision History

Sep. 23, 1997 Updated copyright statement

Aug. 30, 1996 Information previously in the README was inserted into the advisory. Updated version number of AUSCERT checklist and the appendix.

Sep. 20, 1995 Sec. III.A.1 - corrected the command and explanation for checking your configuration.

Sec. III.B.1 - corrected commands for verifying ownership and group membership.

Sec. III.B.2 - replaced this section, which was incorrect.

Sec. III.B.3 - replaced the text and command.

Sec. III.C - added this section, which contains Sun patch information.

Appendix - corrected item 10.

Updates section - added a note about the file name.

10 CA-1995-10: Ghostscript Vulnerability

Original issue date: August 31, 1995
Last revised: September 23, 1997
Updated copyright information

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

A large portion of the technical content of this advisory was provided by the DFN-CERT and NASIRC response teams, and is used with their permission.

There is a vulnerability in older versions of ghostscript (gs) that enables users to execute commands and thus modify files. This problem involves the -dSAFER option and is present in all versions of ghostscript from 2.6 through 3.22 beta.

We recommend that you apply the solution in Section III below to fix the -dSAFER PostScript code or install the latest version of ghostscript (version 4.01). In both cases, we urge you to make -dSAFER the default mode for all versions of ghostscript starting with version 2.6.

We will update this advisory as we receive additional information. Please check advisory files regularly for updates that relate to your site.

I. Background

The PostScript language, which was designed for the expression of graphical data, is widely used for transferring images and preformatted text across the Internet. The language includes primitives for file operations, which were intended to be useful in the expression of images. Unfortunately the operations can be abused by people intentionally embedding commands within an otherwise harmless image so that when displaying that image the PostScript viewer may perform malicious file creations or deletions.

This is a potentially serious problem because many images transferred on the World Wide Web are sent in PostScript. For example, a malicious person could install a booby-trapped image on a web-page, buried among useful or interesting data.

The viewer "ghostscript," a PostScript interpreter, recognizes the command-line option: "-dSAFER". This option is intended to disable the file operations and the %pipe PostScript operator that could be abused to do damage. This option is intended to protect you from this type of sabotage when viewing images from untrusted sources.

II. Problem Description

Problems exist with the ghostscript program, which supports the kind of commands discussed above.

Older versions of ghostscript do not completely disable the pipe operator that can be used execute commands that can modify files. Therefore the option -dSAFER does not provide full protection.

This problem is present in all versions of ghostscript between 2.6 (when the %pipe operator was added) and 3.22beta (when a fix was made).

III. Impact

Attackers who have inserted malicious code into a PostScript file can cause commands to be executed and files to be modified on any system where that PostScript file is viewed with ghostscript.

IV. Solutions

We recommend either fixing the -dSAFER PostScript code or installing version 4.01 of ghostscript (see Sections IV.A and IV.B). In addition, we urge you to enable the -dSAFER option as the default (see Section IV.C).

A. Fixing the -dSAFER PostScript code

The following fix is in the form of "diff" output, which is suitable for use with the GNU patch program. This patch brings the code into conformance with the version of gs_init.ps distributed with the latest version of ghostscript (4.01) and can be applied to the GNU versions 2.6, 2.6.1, and 2.6.2. The file to be patched is in the ghostscript library. As an example, gs_init.ps could be installed in:

```
/usr/local/lib/ghostscript/gs_init.ps
```

Here is the patch. Please see the Updates section at the end of this file for cautions and for corrections to be applied in some situations.

```
--------------------------------cut here--------------------------------------
*** gs_init.ps.orig     Fri Aug 25 10:42:51 1995
--- gs_init.ps  Fri Aug 25 11:16:24 1995
***************
*** 302,308 ****
% If we want a "safer" system, disable some obvious ways to cause havoc.
  SAFER not { (%END SAFER) .skipeof } if
  /file
!  { dup (r) eq
      { file }
      { /invalidfileaccess signalerror }
```

```
     ifelse

--- 302,308 ----

% If we want a "safer" system, disable some obvious ways to cause havoc.

  SAFER not { (%END SAFER) .skipeof } if

  /file

! { dup (r) eq 2 index (%pipe*) .stringmatch not and

      { file }

      { /invalidfileaccess signalerror }

     ifelse

--------------------------------cut here--------------------------------------
```

The key is to change the line that says:

```
{ dup (r) eq
```

to one that says:

```
{ dup (r) eq 2 index (%pipe*) .stringmatch not and
```

Here are the relevant lines in the gs_init.ps file for version 2.6.2 of ghostscript before the patch:

```
302  % If we want a "safer" system, disable some obvious ways to cause havoc.
303  SAFER not { (%END SAFER) .skipeof } if
304  /file
305   { dup (r) eq
306      { file }
307      { /invalidfileaccess signalerror }
308     ifelse
309   } bind odef
310  /renamefile { /invalidfileaccess signalerror } odef
311  /deletefile { /invalidfileaccess signalerror } odef
312  %END SAFER
```

Here are the same lines after the patch has been applied:

```
302  % If we want a "safer" system, disable some obvious ways to cause havoc.
303  SAFER not { (%END SAFER) .skipeof } if
304  /file
305  { dup (r) eq 2 index (%pipe*) .stringmatch not and
306      { file }
307      { /invalidfileaccess signalerror }
308     ifelse
309   } bind odef
310  /renamefile { /invalidfileaccess signalerror } odef
311  /deletefile { /invalidfileaccess signalerror } odef
312  %END SAFER
```

B. Installing version 4.01

You may wish to install Aladdin Ghostscript version 4.01. The latest version of ghostscript is version 4.01 and is available at the locations noted below.

This version of ghostscript is provided by Aladdin Enterprises and is subject to their licensing agreements. Please read the "Aladdin Ghostscript Free Public License" (included in the source code distribution) which differs from the "GNU Public License."

Please note that this version is not the GNU version. The latest GNU version, which is version 2.6.2, does not fix this problem.

ftp://ftp.cs.wisc.edu/ghost/aladdin/ghostscript-4.01.tar.gz
MD5=21a0fe505bbaf75e2e6aeb4e07689fb6

ftp://ftp.cs.wisc.edu/ghost/aladdin/ghostscript-4.01jpeg.tar.gz
MD5=5360e0aa47b415daa44623196f7e6160

ftp://ftp.cs.wisc.edu/ghost/aladdin/ghostscript-4.01zlib.tar.gz
MD5=8eb230a39275b0759f06fa100250fc00

Optionally, you may need the font files for this release. They are available at these locations:

ftp://ftp.cs.wisc.edu/pub/aladdin/ghostscript-fonts-std-4.01.tar.gz
MD5=1e0fe2149affd80deaaae144227049b9

ftp://ftp.cs.wisc.edu/pub/aladdin/ghostscript-fonts-other-4.01.tar.gz
MD5=afe46faf7fde6518ae004a7e8d9a4af4

C. Making -dSAFER the default

To make -dSAFER the default mode for ghostscript for all versions of ghostscript starting with version 2.6, the file gs_init.ps must again be changed. The PostScript commands which check the actual interpreted command are collected in one single if statement in the gs_init.ps file. By commenting out the begin and end lines of this if statement, the check is always applied meaning that the -dSAFER option is always enabled.

NOTE: If you make this change, all file and %pipe operations are disabled and cannot be re-enabled.

The lines which must be changed are:

```
  303  SAFER not { (%END SAFER) .skipeof } if
```

and

```
  312  %END SAFER
```

These two lines should be commented out and made to look like this:

```
  303  % SAFER not { (%END SAFER) .skipeof } if
```

and

```
   312  % %END SAFER
```

If you are using ghostscript 2.6.2, the code will look like the following when both patches noted above are installed:

```
302  % If we want a "safer" system, disable some obvious ways to cause havoc.
303  % SAFER not { (%END SAFER) .skipeof } if
304  /file
305  { dup (r) eq 2 index (%pipe*) .stringmatch not and
306      { file }
307      { /invalidfileaccess signalerror }
308     ifelse
309   } bind odef
310  /renamefile { /invalidfileaccess signalerror } odef
311  /deletefile { /invalidfileaccess signalerror } odef
312  % %END SAFER
```

The CERT Coordination Center staff thanks the DFN-CERT and NASIRC response teams for providing a large portion of the technical content of this advisory, and we thank Wolfgang Ley for his assistance.

UPDATES

1. We have received information that some tools that convert PostScript to other formats break when the SAFER option is the default, as recommended in Section III.C above.

   The problem is that these tools need the PostScript /file directive that is disabled when the SAFER option is made the default. To this end, there is a fix from Joern Tellkamp (tellkamp@informatik.uni-hamburg.de), provided by DFN-CERT that defines an UNSAFER option to ghostscript. By default, ghostscript with the fixes listed in Section III.C above sets the SAFER option.

   The following patch changes the SAFER option to the UNSAFER option. By default, SAFER is on but it can be turned off with the -dUNSAFER option to ghostscript. This, too, is applied to the original gs_init.ps file.

```
Begin UNSAFER Patch
*** gs_init.ps          Fri Aug 25 10:42:51 1995
- --- gs_init.ps.unsafer  Fri Oct 20 13:57:37 1995
***************
*** 66,72 ****
     currentdict /OUTPUTFILE undef
   } if
  currentdict /QUIET known   /QUIET exch def
! currentdict /SAFER known   /SAFER exch def
  currentdict /WRITESYSTEMDICT known   /WRITESYSTEMDICT exch def
  % Acquire environment variables.
- --- 66,72 ----
     currentdict /OUTPUTFILE undef
   } if
  currentdict /QUIET known   /QUIET exch def
! currentdict /UNSAFER known /UNSAFER exch def
  currentdict /WRITESYSTEMDICT known   /WRITESYSTEMDICT exch def
  % Acquire environment variables.
***************
*** 299,308 ****
  /.run /run load def
  /run /run0 load def
! % If we want a "safer" system, disable some obvious ways to cause havoc.
! SAFER not { (%END SAFER) .skipeof } if
  /file
!  { dup (r) eq
      { file }
      { /invalidfileaccess signalerror }
     ifelse
- --- 299,308 ----
  /.run /run load def
  /run /run0 load def
! % If we want an "unsafer" system, enable some obvious ways to cause havoc.
! UNSAFER { (%END UNSAFER) .skipeof } if
  /file
! { dup (r) eq 2 index (%pipe*) .stringmatch not and
      { file }
      { /invalidfileaccess signalerror }
     ifelse
***************
```

```
*** 309,315 ****
   } bind odef
  /renamefile { /invalidfileaccess signalerror } odef
  /deletefile { /invalidfileaccess signalerror } odef
! %END SAFER
  % Create the error handling machinery.
  % The interpreter has created the ErrorNames array.
- --- 309,315 ----
   } bind odef
  /renamefile { /invalidfileaccess signalerror } odef
  /deletefile { /invalidfileaccess signalerror } odef
! %END UNSAFER
  % Create the error handling machinery.
  % The interpreter has created the ErrorNames array.
```

End UNSAFER Patch

Once applied, all of the aforementioned tools need to be changed to add the -dUNSAFER option to the rest of the arguments given to gs, the ghostscript interpreter.

2. We received a report that adding any of the above-mentioned patches may cause the gs interpreter to fail (in version 2.6.0). Should this be the case, changing '.stringmatch' to 'stringmatch' fixes this problem (see below). Upgrading to ghostscript version 2.6.1 also will address the problem.

   If you have a problem with

   ```
   ! { dup (r) eq 2 index (%pipe*) .stringmatch not and
   ```

   change to

   ```
   ! { dup (r) eq 2 index (%pipe*) stringmatch not and
   ```

3. Since it is unknown at this time whether the Macintosh and DOS/Windows versions of ghostscript are vulnerable, we suggest that you apply the patch.
4. Version 3.33 with appropriate patches will address the vulnerabilities outlined in advisory CA-95.10. As of Nov. 8, 1995, the most recent release of ghostscript is Version 3.51.

Revision History

```
Sep. 23, 1997  Updated copyright statement
```

Aug. 30, 1996 Information previously in the README was inserted into the advisory, with editing in the Updates section.

Nov. 08, 1995 Updates section - added SAFER and UNSAFER patches and instructions for applying them. Included a note for Macintosh and DOS/Windows users. Noted a recent release of ghostscript version 3.51.

11 CA-1995-11: Sun Sendmail Vulnerability

Sun Sendmail -oR Vulnerability

===

CERT(sm) Advisory CA-95:11
Original issue date: September 19, 1995
Last revised: September 21, 1996
This advisory is superseded by CA-96.20.
A complete revision history is at the end of this file.
Topic: Sun Sendmail -oR Vulnerability

***** SUPERSEDED BY CA-96.20 *****

The CERT Coordination Center has received reports of problems with the -oR option in sendmail. The problem is present in the version of sendmail that is available from Sun Microsystems, Inc. in SunOS 4.1.X, including patches 100377-19 (for SunOS 4.1.3), 101665-04 (for SunOS 4.1.3_U1), and 102423-01 (for SunOS 4.1.4).

This vulnerability is widely known and is currently being actively exploited by intruders.

The CERT staff recommends installing the appropriate patches as soon as they are available from Sun Microsystems. Alternatives are installing a wrapper or installing sendmail version 8.6.12; see Section III for details. (Although sendmail 8.7 recently became available, we have not yet reviewed it.)
We will update this advisory as we receive additional information.
Please check advisory files regularly for updates that relate to your site.

I. Description

There is a problem with the way that the Sun Microsystems, Inc. version of sendmail processes the -oR option. This problem has been verified as existing in the version of sendmail that is in SunOS 4.1.X, including patches 100377-19 (for SunOS 4.1.3), 101665-04 (for SunOS 4.1.3_U1), and 102423-01 (for SunOS 4.1.4).
The -oR option specifies the host, called the mail hub, to which mail should be forwarded when a user on a client of that hub receives mail. This host can be identified with the -oR option on the command line as

```
    -oRhost_name
```

or in the configuration file as:

```
    ORhost_name
```

or by NFS mounting the /var/spool/mail directory from a file server, probably from the mail hub. In this case, the host name of the file server is used as the forwarding host identified as host_name above. All these configurations are vulnerable.

II. Impact

By exploiting the vulnerabilities, local users may be able to gain unauthorized root access and subsequently read any file on the system, overwrite or destroy files, or run programs on the system. Remote users cannot exploit this vulnerability.

III. Solutions

A. Install a patch from Sun Microsystems.

Check with your local SunService and SunSoft Support Services organizations or SunSolve Online at the URL
http://sunsolve1.sun.com

B. Install the sendmail wrapper available from

ftp://info.cert.org/pub/tools/sendmail/sendmail_wrapper
ftp://ftp.cs.berkeley.edu/pub/sendmail/sendmail_wrapper.c
ftp://ftp.auscert.org.au:/pub/auscert/tools/sendmail_wrapper.c
MD5 = f4049cc56075ddb142f5bd70a53ba341

If you already have this wrapper and are running any version prior to version 1.6, you should immediately upgrade. Details can be found in section 3.1 of AUSCERT advisory (AA-95.09b), available from
ftp://ftp.auscert.org.au/pub/auscert/auscert-advisory

C. An alternative to using the patch or wrapper is to install the latest version of sendmail (as of the issue date of this advisory, it was version 8.6.12) and the sendmail restricted shell program ("smrsh").

1. Install sendmail 8.6.12 or later.

Information on latest versions is available from
ftp://info.cert.org/pub/latest_sw_versions/

Sendmail is available by anonymous FTP from
ftp://ftp.cs.berkeley.edu/ucb/sendmail/
ftp://info.cert.org/pub/tools/sendmail/
ftp://ftp.auscert.org.au/pub/mirrors/ftp.cs.berkeley.edu/ucb/sendmail/
ftp://ftp.cert.dfn.de/pub/tools/net/sendmail/

Checksums for 8.6.12
MD5 (sendmail.8.6.12.base.tar.Z) = 31591dfb0dacbe0a7e06147747a6ccea
MD5 (sendmail.8.6.12.cf.tar.Z) = c60becd7628fad715df8f7e13dcf3cc6
MD5 (sendmail.8.6.12.misc.tar.Z) = 6212390ca0bb4b353e29521f1aab492f
MD5 (sendmail.8.6.12.patch) = 10961687c087ef30920b13185eef41e8
MD5 (sendmail.8.6.12.xdoc.tar.Z) = 8b2252943f365f303b6302b71ef9a841

A note on configuration:
Depending upon the currently installed sendmail program, switching to a different sendmail may require significant effort, such as rewriting the sendmail.cf file. We strongly recommend that if you change to sendmail 8.6.12, you also change to the configuration files that are provided with that version.

In addition, a paper is available to help you convert your sendmail configuration files from Sun's version of sendmail to one that works with version 8.6.12: "Converting Standard Sun Config Files to Sendmail Version 8" by Rick McCarty of Texas Instruments Inc. This paper is included in the sendmail.8.6.12.misc.tar.Z file and is located in contrib/converting.sun.configs.

2. Install the sendmail restricted shell program

To restrict the sendmail program mailer facility, install the sendmail restricted shell program (smrsh) by Eric Allman (the original author of sendmail), following the directions included with the program.

Copies of this program may be obtained from
ftp://info.cert.org/pub/tools/smrsh
ftp://ftp.uu.net/pub/security/smrsh
The checksums are
MD5 (README) = fc4cf266288511099e44b664806a5594
MD5 (smrsh.8) = 35aeefba9714f251a3610c7b1714e355
MD5 (smrsh.c) = d4822ce7c273fc8b93c68e39ec67739c

The CERT Coordination Center thanks AUSCERT for providing the sendmail wrapper.

If you believe that your system has been compromised, contact the CERT Coordination Center or your representative in the Forum of Incident Response and Security Teams (FIRST).

If you wish to send sensitive incident or vulnerability information to CERT staff by electronic mail, we strongly advise that the email be encrypted. The CERT Coordination Center can support a shared DES key, PGP (public key available via anonymous FTP on info.cert.org), or PEM (contact CERT staff for details).

Internet email: cert@cert.org
Telephone: +1 412-268-7090 (24-hour hotline)
CERT personnel answer 8:30 a.m.-5:00 p.m. EST(GMT-5)/EDT(GMT-4), and are on call for emergencies during other hours.
Fax: +1 412-268-6989
Postal address: CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890
USA

CERT advisories and bulletins are posted on the USENET newsgroup comp.security.announce. If you would like to have future advisories and bulletins mailed to you or to a mail exploder at your site, please send mail to cert-advisory-request@cert.org.

Past CERT publications, information about FIRST representatives, and other information related to computer security are available for anonymous

FTP from info.cert.org.

Revision history
Sep. 21, 1996 Superseded by CA-96.20.
Aug. 30, 1996 Information previously in the README was inserted
 into the advisory.
Sep. 25, 1995 Sec. III.B - added note to upgrade if a site is using the
 sendmail wrapper prior to version 1.6. Updated
 pointers and checksum.

12 CA-1995-12: Sun 4.1.X Loadmodule Vulnerability

Original issue date: October 18, 1995
Last revised: September 23, 1997
Attached copyright statement

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

The CERT Coordination Center has received reports of problems with the *loadmodule(8)* program. An exploitation script is available and has been used by local users to gain root privileges.

The problem is present in SunOS 4.1.X only, and there is a patch available for sun4 architectures.

The CERT staff recommends that you install the appropriate patch as soon as possible and take the steps in Section III.B. to further protect your system.

We will update this advisory as we receive additional information. Please check advisory files regularly for updates that relate to your site.

I. Description

The *loadmodule(8)* program is used by the *xnews(1)* window system server to load two dynamically loadable kernel drivers into the currently running system and to create special devices in the /dev directory to use those modules. These modules and special files are used to provide a SunView binary compatibility mode while running the X11/NeWS windowing system. Because of the way the *loadmodule(8)* program sanitizes its environment, unauthorized users can gain root access on the local machine. A script is publicly available and has been used to exploit this vulnerability.

This problem is present in SunOS 4.1.X only.

II. Impact

Local users can gain root privileges.

III. Solution

The CERT staff recommends that you take the steps described in both A and B below.

A. Obtain and install the appropriate patches according to the instructions included with the patches.

Patches are available through your local Sun Answer Center and by FTP from ftp://sunsolve1.sun.com/pub/patches/100448-03.tar.Z.

```
 Module           Patch ID        Filename
----------       ---------       ---------------
loadmodule       100448-03       100448-03.tar.Z
Checksum:
MD5 (100448-03.tar.Z) = 183a22f0a2f6020f1389b6aeea5ca6c6
```

B. Because, in general, a set-user-id program can lead to security exposures, you should also do at least step 1 below. We recommend doing steps 2 and 3 as well.

The intent of these directions is make the *loadmodule(8)* program work only for the super-user (currently it works for all users because it is set-user-id) and to execute it each time the system boots. By following these directions, users who require SunView binary compatibility will have it available to them.

1. If you do not need SunView binary compatibility, then as root, turn off setuid root on the *loadmodule(8)* program with

```
2.     # /bin/chmod u-s /usr/openwin/bin/loadmodule
```

3. If your users need SunView binary compatibility, you can enable it immediately--that is without having to reboot your system--with the following script.

```
4. -----------------------cut here--8<-----------------------
5. ARCH=`/bin/arch -k`
6. OBJ=/sys/${ARCH}/OBJ
7. LM=/usr/openwin/bin/loadmodule
8. /bin/chmod u-s $LM
9. if [ -f $OBJ/evqmod-${ARCH}.o ]; then
10.  if /usr/etc/modstat | /bin/egrep -s evqmod ; then
11.    echo evq: already loaded
12.  elif $LM evqmod-${ARCH}.o evqload; then
13.    echo evq: loaded
14.  else
15.    echo evq: unable to load module
16.  fi
17.fi
18.if [ -f $OBJ/winlock-${ARCH}.o ]; then
19.  if /usr/etc/modstat | /bin/egrep -s winlock ; then
20.    echo winlock: already loaded
21.  elif $LM winlock-${ARCH}.o winlockload; then
22.    echo winlock: loaded
23.  else
24.    echo winlock: unable to load module
25.  fi
26.fi
27.-----------------------cut here--8<-----------------------
```

As a suggestion, store this script in /tmp/esbc and then execute it as root with:

```
# sh /tmp/esbc
```

28. If you've done step 2 above, the module loadings will disappear the next time you reboot your system. To make them permanent-- that is to make these module loadings occur each time your system is rebooted--add the script to the end of your /etc/rc.local file.

The CERT Coordination Center staff thanks Wolfgang Ley and Sun Microsystems for their support in the development of this advisory.

Revision History

```
Sep. 23, 1997  Updated copyright statement
```

```
Aug. 30, 1996  References to README files were removed because updates are added to the advisories themselves.
```

13 CA-1995-13: Syslog Vulnerability - A Workaround for Sendmail

Original issue date: October 19, 1995
Last revised: September 23, 1997
Updated copyright statement

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

The CERT Coordination Center has received reports of problems with the *syslog(3)* subroutine. To the best of our current knowledge, the problem is present in virtually all versions of the UNIX Operating System except the following:

Sony's NEWS-OS 6.X
SunOS 5.5 (Solaris 2.5)
Linux with libc version 4.7.2, released May 1995

We have received reports indicating that the vulnerability is being exploited with a script that has been written to be used with sendmail.

This advisory includes a workaround that you can use with sendmail. It *does not* include workarounds for any other programs that use the *syslog(3)* subroutine--telnetd, ftpd, httpd, etc.

The CERT Coordination Center recommends installing all appropriate syslog-related patches as soon as they are available from vendors. But, in the meantime, we suggest addressing at least the syslog problem in sendmail by installing sendmail version 8.7.1. We are aware that several workarounds concerning the syslog vulnerability have been published on the Internet, but the CERT staff has not formally evaluated them.

We will update this advisory as we receive additional information. Please check advisory files regularly for updates that relate to your site.

I. Description

The *syslog(3)* subroutine uses an internal buffer for building messages that are sent to the *syslogd(8)* daemon. This subroutine does no range checking on data stored in this buffer. It is possible to overflow the internal buffer and rewrite the subroutine call stack. It is then possible to execute arbitrary programs.

This problem is present in virtually all versions of the UNIX Operating System except the following:

Sony's NEWS-OS 6.X
SunOS 5.5 (Solaris 2.5)
Linux with libc version 4.7.2 released in May, 1995

The *sendmail(8)* program uses the *syslog(3)* subroutine, and a script has been written and is being used to exploit the vulnerability.

II. Impact

Local and remote users can execute commands. Prior access to the system is not needed. Exploitation can lead to root access.

III. Solution

We recommend that you do all of A, B, and C.

A. Install syslog patches from your vendor when they become available.

Information we received from vendors as of the issue date of this advisory is attached as Appendix A. We will update the appendix as vendors send updated information.

When you install patches, you will need to recompile/relink any programs built on your system that have been compiled without shared libraries, that is, compiled statically. Be especially careful of programs that contain their own versions of the *syslog(3)* subroutine. You may need to do significant extra work to compile those programs to use the vendor-supplied patches.

B. Install sendmail version 8.7.1.

NOTE: This workaround addresses the *syslog(3)* vulnerability in sendmail only. The vulnerability still exists in all other programs that use *syslog(3)*.

When your vendor(s) provides a patch, we recommend that you rebuild sendmail version 8.7.1 with the patched *syslog(3)* and place that newly compiled version into service.

Sendmail is available by anonymous FTP from

ftp://ftp.cert.org/pub/tools/sendmail/
ftp://ftp.cs.berkeley.edu/ucb/sendmail/
ftp://ftp.auscert.org.au/pub/mirrors/ftp.cs.berkeley.edu/ucb/sendmail/
ftp://ftp.cert.dfn.de/pub/tools/net/sendmail/

Checksum:

MD5 (sendmail.8.7.1.tar.Z) = 4a66d07a059d1d5af5e9ea53ff1b396a

Depending upon your currently installed sendmail program, switching to a different sendmail may require significant effort (such as rewriting the sendmail.cf file). See Section VI for additional notes on installation.

In addition, Sections IV and V below contain scripts for building sendmail 8.7.1 for SunOS 4.1.X and Solaris 2.X, respectively.

C. Install smrsh.

To restrict the sendmail program mailer facility, install and use the sendmail restricted shell program (smrsh). We recommend that you do this regardless of whether you use the vendor's supplied sendmail or you install sendmail version 8.7.1.

Smrsh is now included in the sendmail 8.7.1 distribution in the subdirectory smrsh. See the RELEASE_NOTES file for a description of how to integrate smrsh into your sendmail configuration file.

Please note that although smrsh does not address the vulnerability described in this advisory, a description of smrsh is provided for completeness. We recommend that you install and use smrsh with *all* versions of sendmail.

IV. Building this package for SunOS 4.1.X

Here is a script that is given as an illustration of how to build sendmail 8.7.1 for SunOS 4.1.X. Please refer to READ_ME in the src subdirectory for a more complete explanation of other options available during the compilation process.

```
% uname -sr
SunOS 4.1.2
% ls
sendmail.8.7.1.tar.Z
% zcat sendmail.8.7.1.tar.Z | tar xf -
% cd sendmail-8.7.1/src
% ./makesendmail LIBS='-lresolv' DBMDEF='-DNDBM -DNIS' \
   INCDIRS= LIBDIRS= sendmail
  Configuration: os=SunOS, rel=4.1.2, rbase=4, arch=sun4, sfx=
  Creating obj.SunOS.4.1.2.sun4 using Makefile.SunOS
  Making dependencies in obj.SunOS.4.1.2.sun4
  Making in obj.SunOS.4.1.2.sun4
  ...
```

See Section VI for final installation steps.

V. Building this package for Solaris 2.X

Here is a typescript that is given as an illustration for how to build sendmail 8.7.1 for Solaris 2.X. Note that this procedure assumes that you have the GNU gcc system. The examples below used gcc version 2.6.3. Again, please refer to READ_ME in the src sub-directory for a more complete explanation of other options available during the compilation process.

```
% uname -sr
SunOS 5.4
% ls
```

```
sendmail.8.7.1.tar.Z
% zcat sendmail.8.7.1.tar.Z | tar xf -
% cd sendmail-8.7.1/src
% ./makesendmail LIBS='-lresolv -lsocket -lnsl -lelf' \
    INCDIRS= LIBDIRS= sendmail
  Configuration: os=SunOS, rel=5.4, rbase=5, arch=sun4, sfx=
  Creating obj.SunOS.5.4.sun4 using Makefile.SunOS.5.4
  Making dependencies in obj.SunOS.5.4.sun4
  ...
```

Note: If you wish sendmail version 8.7.1 to use the aliases and configuration file directory conventions from SunOS 5.4, use the following command:

```
./makesendmail LIBS='-lresolv -lsocket -lnsl -lelf' \
ENVDEF='-DSOLARIS=204 -DUSE_VENDOR_CF_PATH' INCDIRS= \
LIBDIRS= sendmail
```

VI. Final Installation Notes

Sendmail can then be installed and configured with new configuration files as needed. We strongly recommend that if you change to sendmail 8.7.1, you also change to the configuration files that are provided with that version.

Significant work has been done to make this task easier. It is now possible to build a sendmail configuration file (sendmail.cf) using the configuration files provided with this release. Consult the cf/READ_ME file for a more complete explanation. We recommended that you create your configuration files using this method because it provides a technique for incorporating any future changes to sendmail into your configuration files.

In addition, we recommend that you recreate your configuration file (sendmail.cf) using the configuration files provided with 8.7.1.

Finally, for Sun users, a paper is available to help you convert your sendmail configuration files from the Sun version of sendmail to one that works with version 8.7.1. The paper is entitled "Converting Standard Sun Config Files to Sendmail Version 8" and was written by Rick McCarty of Texas Instruments Inc. It is included in the distribution and is located in contrib/converting.sun.configs.

Appendix A: Vendor Information

Below is information we have received from vendors concerning the vulnerability described in this advisory. If you do not see your vendor's name, please contact the vendor directly for information.

In addition to vendor information, note that the freely available Linux with libc version 4.7.2, released May 1995, is not vulnerable.

Eric Allman

Neither sendmail version 8.7.3 nor 8.7.1 is vulnerable. Sendmail is available by anonymous FTP from

ftp://ftp.cert.org/pub/tools/sendmail

ftp://ftp.cs.berkeley.edu/ucb/sendmail

ftp://ftp.auscert.org.au/pub/mirrors/ftp.cs.berkeley.edu/ucb/sendmail

ftp://ftp.cert.dfn.de/pub/tools/net/sendmail

MD5 (sendmail.8.7.3.tar.Z) = 3c3891c92500d12d60a61aaa1d01b533

Berkeley Software Design, Inc.

Users of BSD/OS V2.0 and V2.0.1 by Berkeley Software Design, Inc. should install patch U201-001 which works for both versions. The patch is available to all BSDI customers in: ftp://ftp.bsdi.com/bsdi/patches/ md5 checksum: 88b3fd8c83a5926589d7b87b55bc4e14

Convex Computer Corporation

The CERT Coordination Center inadvertently omitted the Convex entry from the original advisory:

Vulnerable: ConvexOS (all releases)

SPPUX (all releases)

A patch is being developed to address this vulnerability in currently supported releases as detailed below. Contact the Convex Technical Assistance Center 1-800-952-0379 to obtain information and patches. There are no known automated attack programs in existence for Convex or SPP architectures. Development of such a program would require access to such a machine, as well as detailed knowledge of the architecture. However, the only completely secure work-around at this time would be to disable sendmail (known to have been successfully attacked on other architectures), as well as other daemons which can potentially log user-supplied strings. Note that the user-supplied strings do not have to actually be routed by syslogd in order for this vulnerability to occur. At this time we do not have a canonical list of affected software; sendmail is the only known-vulnerable agent. It should also be noted that Convex machines make use of a "SPU" workstation (also referred to as a "test station") which controls the machine; these workstations are vulnerable if sendmail is enabled on those workstations and the SPU or test station is located on an accessible network. Convex recommends disabling sendmail on SPU and test-station workstations until a patch can be obtained from Convex.

Currently supported OS releases as of Sep 1, 1995:

ConvexOS 10.1, 10.2, 11.0, 11.1

SPPUX 3.x

Cray Research

Information about fixes for the syslog problem can be found in FN #2011, dated October 10, 1995. Customers should receive this information from their Cray Research service representative. For all source installations, your Cray Research service representative can obtain the fix via the getfix tool. Due to the number of executables which use this library routine, it is not possible to provide getfix packages for all binary installations. UNICOS binary update packages 8.0.4.2 and 9.0.1.2 include this mod. FIX AVAILABILITY as of Feb. 1996.

```
--------------------------------
                         Release Level            Fix Package
Affected Product        Containing Fix           Availability
================        ==============            ===========
UNICOS 8.0             UNICOS 8.0.4.2 *         source only
UNICOS 8.3             **                       source only
UNICOS 9.0             UNICOS 9.0.1.2 ***       source only

*   Released for all platforms.
**  No more updates planned.
*** Released for X-MP, Y-MP, C-90 and T-90 platforms but has not yet
     released for YMP-EL and J-90 platforms.
```

Data General Corporation

The DG/UX operating system is NOT vulnerable to this problem. This includes all currently supported release, DG/UX 5.4 Release 3.00, DG/UX 5.4 Release 3.10, DG/UX Release 4.10 and all related Trusted DG/UX products.

Digital Equipment Corporation

For updated information, please refer to the Digital Equipment Corporation Vendor Bulletin #96.0383, available in ftp://ftp.cert.org/pub/vendors/dec/dec_96.0383.

Note: Non-contract/non-warranty customers should contact local Digital support channels for information regarding these kits.

As always, Digital urges you to periodically review your system management and security procedures. Digital 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.

Hewlett-Packard Company

Included below is information obtained from the February 7th, 1996, Hewlett Packard Security Bulletin, HPSBUX9602-029 "Security Vulnerability in HP-UX *syslog(3)* subroutine." It has been found that all HP-UX systems prior to HP-UX 10.10 have this vulnerability. The vulnerability can be eliminated from releases 9.X and 10.0X of HP-UX by applying a patch. Releases of HP-UX prior to 9.X must upgraded to release 9.X or higher to escape the vulnerability, which is fixed in the HP-UX 10.10 release. There are no work-around solutions known. Hewlett-Packard recommends that all customers concerned with the security of their HP-UX systems either apply the appropriate patch or change perform the actions described above as soon as possible.

Hewlett Packard's HP-UX patches are available via email and World Wide Web.

To obtain a copy of the HP SupportLine email service user's guide, send the following in the TEXT PORTION OF THE MESSAGE to support@us.external.hp.com (no Subject is required):

send guide

The users guide explains the process for downloading HP-UX patches via email and other services available.

World Wide Web service for downloading of patches is available via our URL: (http://us.external.hp.com).

Patches:

PHCO_6595 (series 700/800, HP-UX 10.0 & 10.01), or

PHCO_6598 (series 800, HP-UX 9.0 & 9.04), or

PHCO_6597 (series 700, HP-UX 9.0[1357]), or

PHCO_6224 (series 300/400, HP-UX 9.0, 9.01, 9.03 & 9.1), or

PHCO_6162 (series 700, HP-UX 9.08 BLS), or

PHCO_6161 (series 700, HP-UX 9.09 BLS), or

PHCO_6160 (series 700, HP-UX 9.09+ BLS), or

PHCO_6157 (series 700, HP-UX 10.09 BLS CMW).

Availability:

All patches are available now, except for the BLS patches, which will be available after 29 February, 1996. Contact you FCO representative for patch availability. Further details are provided in Hewlett-Packard Security Bulletin, "HPSBUX9602-029 Security Vulnerability in HP-UX *syslog(3)* subroutine." World Wide Web service for browsing of bulletins is available via our URL: http://us.external.hp.com Choose "Support news", then under Support news, Choose "Security Bulletins"

IBM Corporation

Both fixes are now currently available. Please reference the following fixes:

AIX 4.1 - IX53718

AIX 3.2 - IX53358

Open Software Foundation

OSF cannot reproduce the security hole in OSF/1. However we have reproduced the problem with *syslog(3)*. We have a fix for the *syslog(3)* problem. Support customers should contact OSF for the fix. The fix will be included in the OSF/1 R1.3.2 update release.

The Santa Cruz Operation (SCO)

The "SCO Networking Maintenance Supplement for SCO OpenServer 5" addresses the syslog() problem for all ELF binaries in the product.

This supplement is available in: ftp://ftp.sco.COM/Supplements/net100/.

This includes all the standard network utilities that are often the target of a syslog() attack, such as sendmail. The product also includes a few COFF binaries that use syslog(). These binaries will be corrected in an upcoming Supplement.

Silicon Graphics Inc.

Silicon Graphics released Security Advisory 19951001-01-P825 and patch 825 to address the specifics of CERT Advisory CA-95.13. Please note that patch 1146 (Security Advisory 19960203-01-P1146) supersedes patch 825. This patch addresses additional security problems in the "sendmail" program. Please refer to SGI Advisory 19960203-01-P1146 for further information on these additional security problems, and the location and checksums of this patch. Silicon Graphics has continued to investigate the 8lgm reported syslog vulnerability. A review of utilities supplied with the IRIX 5.3, 6.0, 6.0.1 and 6.1 environments that use syslog has been performed. Silicon Graphics has not discovered any syslog vulnerabilities in these utilities.

Past SGI Advisories and security patches can be obtained via anonymous FTP from sgi-gate.sgi.com or its mirror, ftp.sgi.com.

Solbourne (Grumman)

Solbourne 2.5 is not vulnerable.

Sony Corporation

NEWS-OS 6.0.3 and 6.1 are not vulnerable.

Sun Microsystems, Inc.

SunOS 5.5 is not vulnerable.

Sun Microsystems has made the following patches available to address this vulnerability:

```
PATCH #     VERSION                 RELEASED
---------   -----------             ------------
100891-13 - SunOS 4.1.3             Oct 27, 1995 (International)
101558-07 - SunOS 4.1.3_U1          Oct 27, 1995 (International)
102545-04 - SunOS 4.1.4             Nov 16, 1995 (International)
100890-13 - SunOS 4.1.3             Feb 21, 1996 (US only)
101759-04 - SunOS 4.1.3_U1          Feb 21, 1996 (US only)
102544-04 - SunOS 4.1.4             Feb 21, 1996 (US only)
102903-01 - Solaris 2.3             Nov  2, 1995
101945-37 - Solaris 2.4             Feb. 29, 1996
102905-01 - Solaris 2.4_x86         Nov  2, 1995
```

Note also that the following patches:

```
100890-13 - SunOS 4.1.3             Feb 21, 1996 (US only)
101759-04 - SunOS 4.1.3_U1          Feb 21, 1996 (US only)
102544-04 - SunOS 4.1.4             Feb 21, 1996 (US only)
```

require that you contact your Sun Solution Center or other SunSoft authorized service provider (ASP) in the U.S. to obtain a copy of the actual patch. Sun Security Bulletins are available via the security-alert alias (security-alert@sun.com) and on SunSolve (http://sunsolve1.sun.com).

The CERT Coordination Center staff thanks Eric Allman and Wolfgang Ley for their involvement in the development of this advisory, and thanks Karl Strickland and Neil Woods for reporting the vulnerability.

Revision History

Sep. 23, 1997 Updated copyright statement

Aug. 30, 1996 Information previously in the README was inserted into the advisory.

July 05, 1996 Appendix, Digital- Added pointer to updated information.

July 01, 1996 Appendix, SGI - Added additional information

Apr. 17, 1996 Appendix, SCO - Added an entry for SCO

Mar. 29, 1996 Appendix, Sun - Modified the Sun entry

Feb. 27, 1996 Appendix, Hewlett-Packard & Sun - Updated entries

Feb. 06, 1996 Appendix, Allman & Cray - Updated entries

Dec. 19, 1995 Appendix, Digital - Modified Digital entry

Nov. 07, 1995 Appendix, IBM, SGI, Sun - Updated entries

Nov. 07, 1995 Sec. III.C - Added note recommending smrsh though it doesn't address the particular vulnerability described in the advisory

Oct. 27, 1995 Appendix, Convex, Data General Hewlett-Packard, IBM – Added text

14 CA-1995-14: Telnetd Environment Vulnerability

Original issue date: November 1, 1995
Last revised: October 30, 1997
Updated vendor information for Sun.

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

The CERT Coordination Center has been made aware of a vulnerability with some telnet daemons. The daemons affected are those that support RFC 1408 or RFC 1572, both titled "Telnet Environment Option," running on systems that also support shared object libraries.

To determine if your system is potentially vulnerable, refer to the information we have received from vendors which is summarized in Section III below; details are in Appendix A. Note that if you installed a version of David Borman's telnet package that is older than October 23, 1995, your system may be vulnerable even though it was not vulnerable as distributed by the vendor.

If your vendor is not listed, you will need to determine if your system may be vulnerable. First, determine if your telnet daemon is RFC 1408/1572 compliant. One indication that it is compliant is if your *telnet(1)* program supports the "environ" command or your *telnetd(8)* program supports the ENVIRON or NEW-ENVIRON options. Unless you are certain that your telnet daemon is not RFC 1408/1572 compliant, you may wish to assume it is to be safe. Second, determine if your system supports shared libraries. To do this, consult the *ld(1)* manual page. If it describes dynamic or shared objects, your system probably supports shared object libraries. A system is potentially vulnerable if the telnet daemon supports RFC 1408/RFC 1572 and the system supports shared object libraries.

We recommend that you follow your vendor's directions for addressing this vulnerability. Until you can install a patch, we recommend using the workaround in Appendix B below. If you have previously installed David Borman's telnet package on your system, we recommend that you obtain the current version of telnet (see Section III.C).

We will update this advisory as we receive additional information. Please check advisory files regularly for updates that relate to your site.

I. Description

Some telnet daemons support RFC 1408 or RFC 1572, both titled "Telnet Environment Option." This extension to telnet provides the ability to transfer environment variables from one system to another. If the remote or targeted system, the one to which the telnet is connecting, is running an RFC 1408/RFC 1572-compliant telnet daemon *and* the targeted system also supports shared object libraries, then it may be possible to transfer environment variables that influence the login program called by the telnet daemon. By influencing that targeted system, a user may be able to bypass the normal login and authentication scheme and may become root on that system.

Users with accounts on the targeted system can exploit this vulnerability. Users without accounts on that system can also exploit this vulnerability if they are first able to deposit an altered shared object library onto the targeted system. Therefore, a system may be vulnerable to users with and without local accounts.

Not all systems that run an RFC 1408/RFC 1572-compliant telnet daemon and support shared object libraries are vulnerable. Some vendors have changed the trust model such that environment variables provided by the telnet daemon are not trusted and therefore are not used by the login program. Section III contains a summary of information vendors have reported as of the date of this advisory.

II. Impact

Local and remote users can become root on the targeted system.

III. Solution

The general solution to this problem is to replace the telnet daemon with one that changes the environment given to the login program. We recommend that you install a patch from your vendor if possible. If this is not possible, we recommend using the workaround in Appendix B until you can install a patch. Finally, if you have previously installed Mr. Borman's telnet package, see Section C for how to get a new version that fixes the vulnerability.

A. Vendor Patches

Below is a summary of the vendors listed in Appendix A of this advisory. More complete information, including how to obtain patches, is provided in the appendix. We will update the appendix as we receive more information from vendors.

If your vendor's name is not on this list, please contact the vendor directly.

REMINDER: If you installed a version of David Borman's telnet package that is older than October 23, 1995, your system may be vulnerable even though it was not vulnerable as distributed by the vendor.

Vendor or Source

Apple Computer
Berkeley Software Design
Cray Research
CYGNUS
Data General
Digital Equipment
FreeBSD
Harris
Hewlett-Packard
IBM Corp.

Linux
MIT-distributed for Athena
NEC
NetBSD
Open Software Foundation
OpenVision
SCO
SGI
Sony Corp.

B. Workaround

Until you can install a patch from your vendor, you can use the workaround provided in Appendix B.

C. If you have installed a previous version of Mr. Borman's telnet package, note that he has fixed this problem in the version available at the following location:

ftp://ftp.cray.com/src/telnet/telnet.95.10.23.NE.tar.Z
MD5 checksum 2e14879a5b0aa6dd855a17fa8a3086cf

Appendix A: Vendor Information

Below is information we have received from vendors. If you do not see your vendor's name below, contact the vendor directly for information.

Apple Computer, Inc.

Apple's A/UX is not vulnerable.

Berkeley Software Design, Inc.

BSDI's BSD/OS is not vulnerable.

Cray Research, Inc.

Cray's UNICOS is not vulnerable.

CYGNUS Network Security V4 Free Network Release

cns-95q1 is vulnerable. cns-95q4 is not vulnerable.

Customers can use the following URL to obtain the patch:
http://www.cygnus.com/data/cns/telnetdpatch.html

If customers are unable to obtain the patch in this manner or have any questions, send e-mail to kerbask@cygnus.com.

Note that while the URL and patch are already available, there is no link to the page yet. We will add a link once the announcement has been made.

Data General Corporation

Data General believes the DG/UX operating system to be NOT vulnerable to this problem. This includes all supported releases, DG/UX 5.4 Release 3.00, DG/UX 5.4 Release 3.10, DG/UX Release 4.10 and all related Trusted DG/UX releases.

Specifically, telnetd shipped in DG/UX does not support environment options and does not support RFC 1572.

Digital Equipment Corporation

Digital's OSF/1: vulnerable
Digital's ULTRIX: not vulnerable

Digital has corrected this potential vulnerability. Patches containing new images for Digital's OSF/1 platforms are being provided to your normal Digital Support channels beginning October 31 (U.S. time). The kits may be identified as ECO SSRT0367 (telnetd) for DEC OSF/1 V2.0 thru V3.2c

This potential vulnerability is not present on Digital's ULTRIX systems.

Digital distribution of this announcement will be via AES services (DIA, DSNlink FLASH etc.). Digital Equipment Corporation strongly urges Customers to upgrade to a minimum of DEC OSF/1 V3.0, then apply this patch.

FreeBSD

Vulnerable. A patch has been applied to the current development FreeBSD source tree which is not yet released. This patch is slightly modified compared to posted one, i.e. only variables which affects FreeBSD are disabled. It is telnetd patch, not a login wrapper.

For the official patch, location please contact Jordan Hubbard <jkh@FreeBSD.org>.

Harris

Harris Computer Systems Corporation's Night Hawk is not vulnerable.

Hewlett-Packard Company

HP/UX is not vulnerable.

IBM Corporation

AIX is not vulnerable to this attack.

Linux (freely available software; not a vendor)

Debian GNU/Linux (From "Peter Tobias" <tobias@et-inf.fho-emden.de>):
The current version of the Debian GNU/Linux distribution (released 10/27/95) is not vulnerable anymore. All Debian Installations that use a netstd package version prior to v1.21-1 are vulnerable (telnetd is part of the netstd package). netstd-1.21-1 and above are ok.

Patches are available. Peter fixed the bug last week and uploaded the fixed version to our ftp site (ftp.debian.org). Binaries, sources and the diffs against the bsd telnetd can be found there. The URL for the new binary package is:
ftp://ftp.debian.org/debian/debian-0.93/binary/net/netstd-1.21-1.deb.

and the sources and the diff against the bsd telnetd can be found at:
ftp://ftp.debian.org/debian/debian-0.93/source/net/netstd-1.21-1/telnetd.tar.gz
ftp://ftp.debian.org/debian/debian-0.93/source/net/netstd-1.21-1/telnetd.diff.gz

Red Hat Linux (From Erik Troan <ewt@redhat.com>):
Vulnerable. A fix is now available at:
ftp://ftp.redhat.com/pub/redhat-2.0/updates/NetKit-B-0.06-4.i386.rpm
ftp://ftp.pht.com/pub/linux/redhat/redhat-2.0/updates/NetKit-B-0.06-4.i386.rpm

It will also be fixed in the upcoming Red Hat 2.1 release.

Slackware Linux is vulnerable. The fixes are available from:
ftp://ftp.cymru.net/pub/linux/security/in.telnetd.bin.gz
MD5 (in.telnetd.bin.gz) = 300fc2b022f338e32db411d0e14f0bed

ftp://ftp.cymru.net/pub/linux/security/in.telnetd.bin.elf.gz
MD5 (in.telnetd.bin.elf.gz) = a9ed9a0b90b7a62c98c185e9c7970c5e

The CERT Coordination Center has received information that Paul Leyland <plc@sable.ox.ac.uk> has placed patches for Linux on ftp.ox.ac.uk.

Non-US sites may want to obtain the patches from this archive for convenience. However, please note that these patches will only be available for the next few months; at some point they will be removed from this location.

Linux: This consists of a README, a patch for the telnetd source and a compiled telnetd which should be ok for most Slackware distributions and is available from
ftp://ftp.ox.ac.uk/pub/comp/security/software/patches/telnetd/linux.

MD5 (envpatch) = 3dff044bae0ee7076b8dce735e174962
MD5 (telnetd) = ee2146342059ab00b94fae19f9b1ea63
MD5 (README) = 83f8d07a9b9e8f307346d2ac4b8b3f39

MIT-distributed Athena telnet/telnet95

Vulnerable. Patches available in: ftp://aeneas.mit.edu/pub/kerberos/telnet-patch/.

beta4-3.patch is the patch versus the Beta 4 patch level 3 distribution of Kerberos v5.

beta5.patch is the patch versus the Beta 5 distribution of Kerberos V5.

Both patches have been PGP signed by Ted Ts'o <tytso@MIT.EDU> using detached signatures (beta4-3.patch.sig and beta5.patch.sig).

NEC Corporation

Some NEC systems are vulnerable. Here is their vulnerability matrix:

OS	Version	Status
EWS-UX/V(Rel4.0)	R1.x - R6.x	not vulnerable
EWS-UX/V(Rel4.2)	R7.x - R10.x	not vulnerable
EWS-UX/V(Rel4.2MP)	R10.x	vulnerable patch available
UP-UX/V	R2.x - R4.x	not vulnerable
UP-UX/V(Rel4.2MP)	R5.x - R7.x	vulnerable patch available
UX/4800	R11.x	vulnerable patch available

The patches are available through anonymous FTP from ftp://ftp.meshnet.or.jp in the /pub/48pub/security directory. Please refer to the README file in the directory concerning the appropriate patches that should be retrieved.

OS	Version	Patch-ID and Checksums
EWS-UX/V(Rel4.2MP)	R10.x	NECmas001 Results of sum = 760 295
	MD5	NECmas001.COM.pkg) = 588ED562BBDA6AFF45F1910A75C19B30
UP-UX/V(Rel4.2MP)	R5.x	NECu5s001 Results of sum = 22675 293
	MD5	NECu5s001.COM.pkg) = CBBA695079570BE994EDE8D5AD296B38
	R6.x	NECu6s001 Results of sum = 40159 293
	MD5	NECu6s001.COM.pkg) = C891AF03402CFD092B930253DC3CD607
	R7.x	NECu7s001 Results of sum = 65094 295
	MD5	NECu7s001.COM.pkg) = 00BAFAFF4A8FCFFB58FB6F8F94039D14
UX/4800	R11.x	NECmbs002 Results of sum = 34536 295
	MD5	NECmbs002.COM.pkg) = E6ADAAC22C1B32C4180B855C19B49205

Contacts for further information: Email: UX48-security-support@nec.co.jp

NetBSD

NetBSD 1.0 (the last official release) is vulnerable; NetBSD 1.1 (due out in mid-November) will not be. NetBSD-current is not vulnerable, as of a week or so ago.

Patches: A source form patch has been developed. A core team member will have to make source and binary patches available and provide a location for it.

The login-wrapper given in the advisory can be compiled with NetBSD with:

```
cc -static -o login-wrapper login-wrapper.c
```

Open Software Foundation

OSF/1 version 1.3 is not vulnerable.

OpenVision

This is from: Barry Jaspan <bjaspan@cam.ov.com>:

OpenVision has a patch for the telnetd in OpenV*Secure 1.2 and will contact its customers directly.

The Santa Cruz Operation Inc.

SCO is NOT vulnerable.

Silicon Graphics

On November 16, 1995, Silicon Graphics updated their advisory, 19951101-02-P1010o1020, concerning the Telnetd vulnerability.

In the original advisory, 19951101-01-P1010o1020, the patches 1010 and 1020 were indicated for the wrong versions of IRIX. Patch 1010 is for IRIX 6.1 and patch 1020 is for IRIX 5.2, 5.3, 6.0, 6.0.1. The corrections have been made below.

The solution for this issue is a replacement of the telnetd program for those versions that are vulnerable. The following patches have been generated for those versions vulnerable and freely provides them for the community.

IRIX 3.x

This version of IRIX is not vulnerable. No action is required.

IRIX 4.x

This version of IRIX is not vulnerable. No action is required.

IRIX 5.0.x, 5.1.x

For the IRIX operating systems versions 5.0.x, 5.1.x, an upgrade to 5.2 or better is required first. When the upgrade is completed, then the patches described in the next sections "**IRIX 5.2, 5.3, 6.0, 6.0.1, 6.1**" or "**IRIX 6.1**" can be applied.

IRIX 5.2, 5.3, 6.0, 6.0.1

For the IRIX operating system versions 5.2, 5.3, 6.0, and 6.0.1, an inst-able patch has been generated and made available via anonymous ftp and/or your service/support provider. The patch is number 1020 and will install on IRIX 5.2, 5.3, 6.0 and 6.0.1 .

The SGI anonymous ftp site is sgigate.sgi.com (204.94.209.1). Patch 1020 can be found in the following directories on the ftp server:

~ftp/Security

or

~ftp/Patches/5.2
~ftp/Patches/5.3
~ftp/Patches/6.0
~ftp/Patches/6.0.1

The actual patch will be a tar file containing the following files:

```
Filename:                 README.patch.1020
Algorithm #1 (sum -r):    31057 8 README.patch.1020
Algorithm #2 (sum):       40592 8 README.patch.1020
MD5 checksum:             02F06ECD6240015F8DF82A99EC01E911
Filename:                 patchSG0001020
Algorithm #1 (sum -r):    07232 2 patchSG0001020
Algorithm #2 (sum):       47310 2 patchSG0001020
MD5 checksum:             DA2341626FAEB9D67BA85FA3465BA9D9
Filename:                 patchSG0001020.eoe1_sw
Algorithm #1 (sum -r):    22449 62 patchSG0001020.eoe1_sw
Algorithm #2 (sum):       36518 62 patchSG0001020.eoe1_sw
MD5 checksum:             936019F2CC9AB6CAE0D2DF611D461475
Filename:                 patchSG0001020.eoe2_sw
Algorithm #1 (sum -r):    29899 43 patchSG0001020.eoe2_sw
Algorithm #2 (sum):       12088 43 patchSG0001020.eoe2_sw
MD5 checksum:             19A9C0BCB6F178E7EDF86850A1CF81D1
Filename:                 patchSG0001020.idb
Algorithm #1 (sum -r):    64615 2 patchSG0001020.idb
Algorithm #2 (sum):       46761 2 patchSG0001020.idb
MD5 checksum:             487831A62C61FEAF5797859CBC1F018C
```

IRIX 6.1

For the IRIX operating system version 6.1, an inst-able patch has been generated and made available via anonymous ftp and/or your service/support provider. The patch is number 1010 and will install on IRIX 6.1 .

The SGI anonymous ftp site is sgigate.sgi.com (204.94.209.1). Patch 1010 can be found in the following directories on the ftp server:

~ftp/Security

or

~ftp/Patches/6.1

The actual patch will be a tar file containing the following files:

```
Filename:                 README.patch.1010
Algorithm #1 (sum -r):    43949 8 README.patch.1010
Algorithm #2 (sum):       38201 8 README.patch.1010
MD5 checksum:             A8781E18A1F79716FBFE0B6E083DAB31
Filename:                 patchSG0001010
Algorithm #1 (sum -r):    08656 2 patchSG0001010
Algorithm #2 (sum):       45506 2 patchSG0001010
MD5 checksum:             34CF7F63073C225AD76150A4088E76AB
Filename:                 patchSG0001010.eoe1_sw
Algorithm #1 (sum -r):    12843 65 patchSG0001010.eoe1_sw
Algorithm #2 (sum):       42034 65 patchSG0001010.eoe1_sw
MD5 checksum:             82B8D375ECBF58A08286D393CE3980E7
Filename:                 patchSG0001010.eoe2_sw
Algorithm #1 (sum -r):    01655 47 patchSG0001010.eoe2_sw
Algorithm #2 (sum):       19507 47 patchSG0001010.eoe2_sw
MD5 checksum:             1A5C5B5B84E0188A923C48419F716492
Filename:                 patchSG0001010.idb
Algorithm #1 (sum -r):    31514 2 patchSG0001010.idb
Algorithm #2 (sum):       46531 2 patchSG0001010.idb
MD5 checksum:             9540492FEB00D41281AAF90AC3F67FA9
```

SGI Security Information/Contacts:

For obtaining security information, patches or assistance, please contact your SGI support provider. If there are questions about this document, email can be sent to cse-security-alert@csd.sgi.com. For reporting *NEW* SGI security issues, email can be sent to security-alert@sgi.com.

Sony Corporation

Sony's NEWS-OS 6.x is not vulnerable.

Sun Microsystems, Inc.

Versions of Solaris prior to 2.5 and SunOS do not support the "environ" option and are not affected by the reported problem.

Appendix B: login-wrapper Workaround

The login-wrapper program shown below is meant to be executed just before the distributed login program. The wrapper cleans specific variables from the environment before invoking the distributed login program.

```
------------------------cut here--8<------------------------
/*
* This is a login wrapper that removes all instances of
* various variables from the environment.
*
* Note: this program must be compiled statically to be
* effective against exploitation.
*
* Author:      Lawrence R. Rogers
*
* 10/25/95     version 1.1     Original version
* 10/26/95     version 1.2     ELF_ variables removed (Linux)
* 10/27/95     version 1.3     ELF_ changed to ELF_LD_
*                              Added AOUT_LD_ (Linux)
*
*/
#include        <stdio.h>
#if !defined(_PATH_LOGIN)
# define                _PATH_LOGIN     "/bin/login.real"
#endif
main (argc, argv, envp)
int argc;
char **argv, **envp;
{
        register char **p1, **p2;
        for (p1 = p2 = envp; *p1; p1++) {
                if (strncmp(*p1, "LD_", 3) != 0 &&
                    strncmp(*p1, "_RLD", 4) != 0 &&
                    strncmp(*p1, "LIBPATH=", 8) != 0 &&
                    strncmp(*p1, "ELF_LD_", 7) != 0 &&
                    strncmp(*p1, "AOUT_LD_", 8) != 0 &&
                    strncmp(*p1, "IFS=", 4) != 0 ) {
                            *p2++ = *p1;
                }
        }
        *p2 = 0;
        execve(_PATH_LOGIN, argv, envp);
        perror(_PATH_LOGIN);
        exit(1);
}
------------------------cut here--8<------------------------
```

The following two examples show how to compile the login-wrapper for SGI's IRIX 5.3 and FreeBSD 2.x systems. The examples move the distributed login program to a new location and install the wrapper in the standard location. When executed, the wrapper first cleanses the environment and then calls the relocated, distributed login program.

Note 1: The wrapper must be compiled statically. On SGI's IRIX system, compiling statically requires that the non-shared versions of libraries be installed. Consult your system documentation to determine how to do this.

Note 2: You may need to change the _PATH_LOGIN variable to define where the real login program resides on your system. On some systems, login resides in /usr/bin/login.

Compiling for IRIX 5.3

```
# uname -a
IRIX test 5.3 11091812 IP22 mips
# /bin/ls -l /usr/lib/iaf/scheme
- -rwsr-xr-x    1 root     sys        65832 Sep  9 14:24
/usr/lib/iaf/scheme
# /bin/cc -non_shared -O -D_PATH_LOGIN=\"/usr/lib/iaf/scheme.real\"
\
        login-wrapper.c -o login-wrapper
# /bin/mv /usr/lib/iaf/scheme /usr/lib/iaf/scheme.real
# /bin/chmod 755 /usr/lib/iaf/scheme.real
# /bin/mv login-wrapper /usr/lib/iaf/scheme
# /bin/chmod 4755 /usr/lib/iaf/scheme
# /bin/chown root /usr/lib/iaf/scheme
# /bin/chgrp  sys /usr/lib/iaf/scheme
# /bin/ls -lL /usr/lib/iaf/scheme /usr/lib/iaf/scheme.real
- -rwxr-xr-x    1 root     sys        65832 Sep  9 14:24
/usr/lib/iaf/scheme.real
- -rwsr-xr-x    1 root     sys       213568 Oct 30 08:42
/usr/lib/iaf/scheme
```

Compiling for FreeBSD 2.x

```
# /bin/ls -lg /usr/bin/login
- -r-sr-xr-x  1 root  bin  20480 Jun 10 20:00 /usr/bin/login
# /usr/bin/cc -D_PATH_LOGIN=\"/usr/bin/login.real\" -static \
        -O login-wrapper.c -o login-wrapper
# /bin/mv /usr/bin/login /usr/bin/login.real
# /bin/chmod 555 /usr/bin/login.real
# /bin/mv login-wrapper /usr/bin/login
# /bin/chmod 4555 /usr/bin/login
# /usr/sbin/chown root.bin /usr/bin/login
# /bin/ls -lg /usr/bin/login /usr/bin/login.real
- -r-sr-xr-x  1 root  bin  24885 Oct 25 22:14 /usr/bin/login
- -r-xr-xr-x  1 root  bin  20480 Jun 10 20:00 /usr/bin/login.real
```

The CERT Coordination Center staff thanks Eric Halil of AUSCERT, Wolfgang Ley of DFNCERT, and Sam Hartman of the MIT Kerberos Development team for their support in responding to this problem.

Revision History

Oct. 30, 1997 Updated vendor information for Sun.

Sep. 26, 1997 Updated copyright statement

Aug. 30, 1996 Information previously in the README was inserted into the advisory.

Mar. 22, 1996 Appendix A, SGI - Modified information for Silicon Graphics.

Feb. 08, 1996 Appendix A, NEC - Added patch information.

Nov. 08, 1995 Appendix A, IBM - Added an entry for IBM.

Linux - Added information about Slackware Linux.

NetBSD - Corrected compilation instructions.

SCO - Noted SCO is not vulnerable.

SGI - Updated information.

Sun - Added an entry.

Nov. 08, 1995 Appendix B - Replaced IRIX 5.3 section with new material.

15 CA-1995-15: SGI lp Vulnerability

Original issue date: November 8, 1995
Last revised: September 23, 1997
Updated Copyright statement

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

The CERT Coordination Center has had several security incidents reported to us involving the lp account on the Silicon Graphics, Inc. (SGI) IRIX system. As distributed by SGI, the lp account, as well as other accounts, has no password on a newly installed system. The lp account, which is used by the *lp(1)* program for remote printing, and other accounts are initially configured without passwords to provide easy "plug-and-play" install and operation. However, these password-less accounts are well known by intruders and allow unintended access to your system.

In the documentation that SGI distributes with their systems, these password-less accounts are specifically addressed in the "IRIX Advanced Site and Server Administrative Guide" in the chapter on System Security. The documentation recommends disabling the login for the lp account. It also recommends that you create passwords for the following accounts immediately: demos, guest, lp, nuucp, root, tour, tutor, and 4Dgifts. The documentation includes guidelines for choosing good passwords.

To determine if your system is vulnerable, use the following command as root to display the status of all password-less accounts:

```
# /bin/passwd -sa | /bin/awk '$2 == "NP" {print $0}'
```

If this command displays any accounts, especially the lp account, then your system is vulnerable. To address this vulnerability, we recommend using the workarounds in Section III below.

We will update this advisory as we receive additional information. Please check advisory files regularly for updates that relate to your site.

I. Description

The SGI IRIX system as distributed has some accounts without passwords. Among the accounts that are password-less is the lp account. This account is used in part by the *lp(1)* program to manage object and spooled data files in the /var/spool/lp directory (for IRIX 4.X, this directory is /usr/spool/lp). The account is created without a password because *lp(1)* uses *rsh(1)* to transfer files from print clients to print servers.

II. Impact

Remote users can gain access to systems without authentication. The level of privilege gained depends on the password-less account used to access a system.

Although the scope of this advisory is the lp account, keep in mind that any account without a password (or with an easy-to-guess password) is a point for access without authentication.

III. Solution

The general solution is to lock all accounts that do not have passwords. Section A below describes how to do that.

Section B suggests one way to re-enable print client to print server communication.

A. Lock each password-less account.

Store the following script in /tmp/CheckPasswords for example and then run it as root on your machine to lock each password-less account. The password installed will not allow the accounts to be used as login accounts. See the *passwd(1)* manual page for more details. Note that this script only locks accounts on the local machine. If there are password-less accounts in NIS, those accounts will not be locked by this script.

```
------------------------cut here--8<-----------------------
#!/bin/sh
for account in `/bin/passwd -sa | /bin/awk '$2 == "NP" {print $1}'`
do
        /bin/echo Locked the $account account
        /bin/passwd -l $account
done
------------------------cut here--8<-----------------------
```

The first time the script is run, it should display something similar to the following:

```
        # sh /tmp/CheckPasswords
        Locked the tutor account
        Locked the tour account
        Locked the lp account
        ...
```

If the script locked an account, run the script again. This time it should produce no output because all password-less accounts have now been locked.

B. Re-enable print client to print server communication.

(We have verified with SGI that you can use the script in this section to re-enable the print client to print server communication. SGI has asked us to make it clear, however, that they do not have the resources to handle issues relating to the use of wrappers.)

Note that, in general, the CERT Coordination Center recommends that the rlogin and rsh services be blocked at your Internet routers and turned off on all of your machines. If you have turned the rsh service off on your print server, you will need to turn it back on on that machine. If you decide to do this, we strongly recommend that you install and use a TCP/IP wrapper program to restrict the set of machines that can connect to your print server's rsh service. A TCP/IP wrapper program is available from ftp://ftp.cert.org/pub/tools/tcp_wrappers/tcp_wrappers_7.2.tar.Z
MD5 (tcp_wrappers_7.2.tar.Z) = 883d00cbd2dedd9bfc783b7065740e74

Once the rsh service is turned on on your print server and a TCP/IP wrapper program installed and configured, you then need to define the set of machines that can communicate with your print server.

For each IRIX system that controls a printer, the lp account needs to be changed to re-enable print client to print server communication. To do this, the lp account on each print server needs a .rhosts file in lp's home directory, typically /var/spool/lp (for IRIX 4.X, this directory is /usr/spool/lp). The owner and group of this file must be the same as that of the lp account. Its contents are lines of the form:

```
        print_client_name       lp
```

Each line identifies the name of the print client and indicates that the lp account is the account that is allowed to rsh from the print client to the print server.

The following shows an example of configuring communication from a print client (named "client") to a print server. This configuration need only be done on a print server. The ping command is used to determine the print client's formal name according to whatever host resolution scheme is in place. That name is stored in the .rhosts file. The last two lines, the ping and the echo, need to be repeated for each client of a print server.

```
# /bin/awk -F: '$1 == "lp" {print $0}' /etc/passwd
lp:*LK*:9:9:Print Spooler Owner:/var/spool/lp:/bin/sh
# cd `/bin/awk -F: '$1 == "lp" {print $6}' /etc/passwd`
# /bin/touch .rhosts
# /bin/chown lp .rhosts
# /bin/chgrp lp .rhosts
# /bin/chmod 600 .rhosts
# /usr/etc/ping -c 1 client | /bin/awk '$1 == "PING" {print $2}'
client.YourDomain
# /bin/echo client.YourDomain lp >> .rhosts
```

The CERT Coordination Center staff thanks Silicon Graphics Inc. and Christopher Kranz of Princeton University for their support in responding to this problem.

UPDATES

Silicon Graphics, Inc. have issued a Security Advisory concerning this vulnerability (19951002-01-I). Their advisory can be obtained from ftp://sgigate.sgi.com/security.

We have received additional information from one member of our constituency regarding the vulnerability in the SGI printing system and the accounts without passwords. The supercomputer NEC SX-3 running "SUPER-UX unix 5.10 1 SX-3" (which is very similar to IRIX) also has the same vulnerability.

(As far as we are aware there are only about 30 machines [in the world] running this OS.)

Revision History

Sep. 23, 1997 Updated copyright statement

Aug. 30, 1996 Information previously in the README was inserted into the advisory.

Dec. 20, 1995 Updates section - Added a pointer to SGI advisory and a note about the supercomputer NEC SX-3.

16 CA-1995-16: wu-ftpd Misconfiguration Vulnerability

Original issue date: November 30, 1995
Last revised: September 23, 1997
Updated copyright statement

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

A vulnerability exists with certain configurations of the SITE EXEC command in the Washington University ftpd, also known as wu-ftpd. Exploitation of this vulnerability may allow root access from any account on the system.

The vulnerable configuration is known to exist in numerous Linux distributions and is currently being actively exploited by intruders.

It should be noted that this vulnerability is not necessarily limited to Linux but may exist on any wu-ftpd installation. Thus, all users of the wu-ftpd program, not just the Linux users, should take this opportunity to verify the configuration of their daemons. Note that versions of wu-ftpd before the 2.4 release contain serious security vulnerabilities and should be updated immediately.

Section III contains instructions for disabling ftpd and correcting the configuration.

We will update this advisory as we receive additional information. Please check advisory files regularly for updates that relate to your site.

I. Description

There is a problem with the default configuration of the Washington University FTP Server version 2.4 in major Linux distributions, including but not limited to Slackware 2.0, 2.1, 2.2, 2.3, Yggdrasil Plug&Play Fall'94, and the Debian Distribution. By exploiting this problem, any user who is able to log into a system having the vulnerable configuration via FTP using their login, and not the anonymous login, may gain root access.

Other systems besides Linux can be configured to be vulnerable although the standard wu-ftpd 2.4 source code as distributed is not vulnerable.

The problem is that the variable _PATH_EXECPATH was set to "/bin" in the configuration file src/pathnames.h when the distribution binary was built. _PATH_EXECPATH should be set to "/bin/ftp-exec" or a similar directory that does not contain a shell or command interpreter, for example. The source code shipped with the Linux distributions contains the correct value ("/bin/ftp-exec") despite the incorrect distribution binary. You should verify that _PATH_EXECPATH has the correct value before recompiling.

Note that the documentation for wu-ftpd states that the directory defined by _PATH_EXECPATH is relative to ~ftp, the ftp home directory as specified in the password file. This is misleading. The pathname is relative to ~ftp for anonymous users only. This pathname is relative to "/" for other user sessions.

II. Impact

Any user with a local account on a system offering FTP services with the vulnerable configuration may gain root access. Support for anonymous FTP access is not required to exploit this vulnerability.

III. How to determine if you are vulnerable

All systems running wu-ftpd should be checked to determine if the configuration is vulnerable.

To test your configuration, access the FTP server using a legitimate user account (not an anonymous FTP login) and login to your FTP server. For example:

```
    srchost> ftp ftphost
    Connected to ftphost
    220 ftphost FTP server (Version wu-2.4(2) Mon Apr 18 09:135
[...]
    ready.
    Name (srchost:joe):
    331 Password required for joe.
    Password:
    230 User joe logged in.
```

Then type:

```
    ftp> quote site exec echo problem
```

If you see the following response, then you are not vulnerable:

```
    200-echo problem
    200  (end of 'echo problem')
```

However, if you see this following response, then you are vulnerable (note the additional '200-problem' entry):

```
    200-echo problem
    200-problem
    200  (end of 'echo problem')
```

IV. Solution

If you have the vulnerability, we recommend that you turn off ftpd immediately using the method described in Section A below. Once you have done that, you can then decide whether to rebuild or fetch a new ftpd binary.

If you have built wu-ftpd from a source distribution, follow the steps in Sections B.2 and B.3 below.

Once you have eliminated this vulnerability, turn on ftpd with the method described in Section C below.

A. Disable ftpd

To disable ftpd, do the following as root.

1. Shut down the FTP server using the ftpshut command. This command blocks all connections to the FTP server.

   For ftpshut to work correctly, the *ftpaccess(5)* file will need a shutdown directive that names a file used by wu-ftpd to indicate that the server is shutdown. If your ftpaccess file does not have such a directive, add one to that file. When added, use *ftpshut(8)* to shut down the server. Once the server has been shutdown, all new incoming FTP requests will fail.

   Here is an example of the ftpshut command:

   ```
   ftpshut now
   ```

2. Verify that the FTP service has been shut down by attempting to connect to it. You should see a message that contains a line similar to the following:

   ```
   hostname FTP server shut down -- please try again later
   ```

   where hostname is the host from which you are requesting FTP service.

B. Correct the configuration

Item 1 below applies to those running Debian Linux. Item 2 applies to all other Linux systems. Item 3 applies to those who are building wu-ftpd from source on systems other than Linux.

1. If you are running Debian Linux, obtain a fixed binary, available from the following location, and install this binary.

   ftp://ftp.debian.org/debian/debian-0.93/binary/net/wu-ftpd-2.4-14.deb
   MD5 (wu-ftpd-2.4-14.deb) = c00a0aac75216bf83568aee4c2e7d168

2. If you are running any version of Linux, there is a version of the source code available that has been improved to compile more cleanly. It too is correctly configured for SITE EXEC. It is available from (file wu-ftpd-2.4-fixed.tar.gz)

   ftp://bach.cis.temple.edu/pub/Linux/security/wu-ftpd-2.4-fix/
   MD5 (wu-ftpd-2.4-fixed.tar.gz) = 3e1c6fd7cd6757e45894df0d3638b524

   This version is also correctly configured for the SITE EXEC command and can be compiled and installed. Consult Section IV below for suggestions on how to configure wu-ftpd.

3. If you are running a version of wu-ftpd before version 2.4, you should upgrade to version 2.4 first. That version is available from

ftp://wuarchive.wustl.edu/packages/wuarchive-ftpd/wu-ftpd-2.4.tar.Z
MD5 (wu-ftpd-2.4.tar.Z) = 57f1a962c90a9b12825d39af518df433

Version 2.4 is correctly configured for the SITE EXEC command and can be compiled and installed. Consult Section IV below for suggestions on how to configure wu-ftpd.

C. Enabling ftpd

1. To turn ftpd back on, delete the file referenced by the shutdown directive in your ftpaccess file.
2. Verify that the FTP service has been enabled by attempting to connect to it. You should see a message that contains lines similar to the following:

```
srchost> ftp ftphost
Connected to ftphost
220 ftphost FTP server (Version wu-2.4(3) Mon Apr 3 16:53:11
EDT 1995) ready.
Name (srchost:joe):
```

IV. Advice on configuring the FTP Daemon for SITE EXEC

Here are some configuration guidelines for the directories named by the _PATH_EXECPATH variable.

1. Directories used by SITE EXEC: The documentation for wu-ftpd states that the directory defined by the _PATH_EXECPATH variable is relative to ~ftp, the ftp home directory as specified in the password file. This is misleading. The pathname is relative to ~ftp for anonymous users only. The pathname is relative to "/" for all other user sessions.

   Therefore, you need to check the two directories used by the SITE EXEC command. For example, if the _PATH_EXECPATH variable is set to /bin/ftp-exec, then wu-ftpd searches the ~ftp/bin/ftp-exec directory for programs specified by SITE EXEC when the anonymous login is used, and the /bin/ftp-exec directory specified by SITE EXEC when any other login is used.

2. Contents of the directories used by SITE EXEC: The commands installed in these directories can be executed by the SITE EXEC command. We strongly recommend that this directory contain only those programs that you wish to be executed by those users who connect to your FTP server. An example of a program to install in these directories is the ls program. Programs that should not be installed in these directories are shells, for example sh or csh, and command interpreters, for example awk and perl.

The CERT Coordination Center thanks AUSCERT, the Australian response team, and Alexander O. Yuriev, Temple University, author of Linux Security Updates, for their support in responding to this problem. Linux Security Updates are available from http://bach.cis.temple.edu/linux/linux-security/

UPDATES

Information for Solaris 2.4

After the advisory was originally issued, Charles Jardine <cj10@cam.ac.uk> provided the following information.

The problem with the SITE EXEC command is that programs spawned by wu-ftpd are run as the effective user and group id of the logged in user but real user and group id of root (or however wu-ftpd is started by inetd, usually root).

To address this, the following can be used as a basis for a patch. (Note that this patch works for Solaris 2.4 compiled with gcc-2.7.2.)

```
*** /tmp/T0a001YI       Mon Dec  4 10:22:13 1995
--- popen.c     Mon Dec  4 10:22:08 1995
***************
*** 141,146 ****
--- 141,158 ----
              }
              (void) close(pdes[1]);
          }
+ /*
+  * This fixes the ``real'' problem with SITE EXEC
+  */
+       {
+               uid_t u = geteuid();
+               gid_t g = getegid();
+
+               setuid(0);
+               setgid(g);
+               setuid(u);
+       }
+
          execv(gargv[0], gargv);
          _exit(1);
      }
```

Revision History

```
Sep. 23, 1997  Updated copyright statement

Aug. 30, 1996  Information previously in the README was inserted
into the advisory.

Jan. 19, 1996  Updates - Added code that can be used as the basis
for a patch for the SITE EXEC command for Solaris 2.4.
```

```
Dec. 19, 1995  Sec. III - Expanded the explanation of how to deter-
mine if you are vulnerable.
```

17 CA-1995-17: rpc.ypupdated Vulnerability

Original issue date: December 12, 1995
Last revised: October 30, 1997
Updated vendor information for Sun.

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

The CERT Coordination Center has received reports of a vulnerability in the rpc.ypupdated program. An exploitation program has also been posted to several newsgroups.

This vulnerability allows remote users to execute arbitrary programs on machines that provide Network Information Service (NIS) master and slave services. Client machines of an NIS master or slave server are not affected.

See Section III for a test to help you determine if you are vulnerable, along with a workaround. In addition, Appendix A contains a list of vendors who have reported their status regarding this vulnerability.

We will update this advisory as we receive additional information. Please check advisory files regularly for updates that relate to your site.

I. Description

The rpc.ypupdated program is a server used to change NIS information from a network-based client using various methods of authentication.

Note:
The Network Information Service (NIS) was formerly known as Sun Yellow Pages (YP). The functionality of the two remains the same; only the name has changed. The name Yellow Pages is a registered trademark in the United Kingdom of British Telecommunications plc, and may not be used without permission.

Clients connect to rpc.ypupdated and provide authentication information and proposed changes to an NIS database. If authenticated, the information provided is used to update the selected NIS database.

The protocol used when clients communicate with a server only checks to see if the connection is authentic using secure RPC. The protocol does not check to see if the client is authorized to modify the NIS data or if the given NIS map exists. Even after an unsuccessful attempt to update the NIS information, the rpc.ypupdated server invokes the *make(1)* program to propagate possible changes. The invocation of make is implemented in an insecure fashion which allows the requesting client to pass malicious arguments to the call resulting in the execution of arbitrary commands on NIS master and slave servers.

II. Impact

Remote users can execute commands on vulnerable NIS master and slave machines.

III. Solution

First determine if you are vulnerable (see Sec. A below). If you are vulnerable, either follow the instructions vendors have provided in Appendix A or apply the workaround in Sec. B below.

A. Consult the vendor information in Appendix A.

If your vendor is not listed, then check to see if your system has an rpc.ypupdated server. To do this check, consult your system documentation or look in your system initialization files (e.g., /etc/rc*, /etc/init.d/*, and inetd.conf) for rpc.ypupdated or ypupdated. If you find a reference to this program on your system, then it is likely that you are vulnerable.

B. Until patches are available for vulnerable systems, we recommend that you disable rpc.ypupdated as soon as possible.

Below are some examples given for reference only. Consult your system documentation for the exact details.

In these examples, the rpc.ypupdated program is killed if it is running, and the system is reconfigured so that the daemon does not automatically start again when the system is rebooted.

Example 1 - SunOS 4.1.X
For SunOS 4.1.X master and slave NIS servers, the rpc.ypupdated program is started by the /etc/rc.local script. First, determine if the server is running, and kill it if it is. Then, rename rpc.ypupdated so that the /etc/rc.local script will not find and therefore start it when the system reboots.

```
# /bin/uname -a
SunOS test-sun 4.1.4 1 sun4m
# /bin/ps axc | /bin/grep rpc.ypupdated
  108 ?  IW    0:00 rpc.ypupdated
# /bin/kill 108
# /bin/ps axc | /bin/grep rpc.ypupdated
# /bin/grep ypupdated /etc/rc /etc/rc.local
/etc/rc.local:  if [ -f /usr/etc/rpc.ypupdated -a -d
/var/yp/$dname ]; then
/etc/rc.local:          rpc.ypupdated;  echo -n ' ypupdated'
# /bin/mv /usr/etc/rpc.ypupdated /usr/etc/rpc.ypupdated.CA-95.17
# /bin/chmod 0 /usr/etc/rpc.ypupdated.CA-95.17
```

Example 2 - IRIX
On IRIX systems, ypupdated is started by the inetd daemon. For versions 3.X, 4.X, 5.0.X, 5.1.X, and 5.2, the ypupdated is enabled; but for versions 5.3, 6.0.X, and 6.1, it is disabled. Note that the byte counts given for /bin/ed may vary from system to system. Note also that the inetd.conf file is found in different locations for different releases of IRIX. For 3.X and 4.X, it is located in /usr/etc/inetd.conf. For all other releases (5.0.X, 5.1.X, 5.2, 5.3, 6.0.X, and 6.1) it is in /etc/inetd.conf.

```
# /bin/uname -a
IRIX test-iris 5.2 02282015 IP20 mips
# /bin/grep ypupdated /etc/inetd.conf
ypupdated/1 stream rpc/tcp wait root /usr/etc/rpc.ypupdated
ypupdated
# /bin/ps -eaf | /bin/grep rpc.ypupdated
    root   184     1  0   Nov 20 ?        0:00
/usr/etc/rpc.ypupdated
    root 14694 14610  2 11:30:07 pts/3    0:00 grep -i
rpc.ypupdated
# /bin/kill 184
# /bin/ed /etc/inetd.conf
3344
/^ypupdated/s/^/#DISABLED# /p
#DISABLED# ypupdated/1 stream rpc/tcp wait root
/usr/etc/rpc.ypupdated ypupdated
w
3355
q
# /bin/ps -eac | /bin/grep inetd
   193   TS  26 ?        0:04 inetd
# /bin/kill -HUP 193
```

Appendix A: Vendor Information

Below is information we have received from vendors. If you do not see your vendor's name below, please contact the vendor directly for information.

Apple Computer, Inc.

A/UX does not include this functionality and is therefore not vulnerable.

Berkeley Software Design, Inc. (BSDI)

BSD/OS by Berkeley Software Design, Inc. (BSDI) is not vulnerable.

Data General Corporation

Data General believes the DG/UX operating system to be NOT vulnerable. This includes all supported release, DG/UX 5.4 Release 3.10, DG/UX Release 4.10 and all related Trusted DG/UX releases.

Digital Equipment Corporation

OSF/1 on all Digital platforms is not vulnerable.

Digital ULTRIX platforms are not vulnerable to this problem.

Hewlett-Packard Company

HP-UX versions 10.01, 10.10, and 10.20 are vulnerable (versions prior to HP-UX 10.01 are not vulnerable).

Solution: Do not run rpc.ypupdated. rpc.ypupdated is used when adding or modifying the public:private key pair in the NIS map public key.byname via the chkey command interface. rpc.ypupdated should ONLY be run while changes are being made, then terminated when the changes are complete.
Make sure you re-kill rpc.ypupdated after each reboot.

IBM Corporation

AIX 3.2

APAR - IX55360
PTF - U440666

To determine if you have this PTF on your system, run the following command:

```
lslpp -lB U440666
```

AIX 4.1

APAR - IX55363

To determine if you have this fix on your system, run the following command:

```
lslpp -h | grep -p bos.net.nis.server
```

Your version of bos.net.nis.server should be 4.1.4.1 or later.

To Order

APARs may be ordered using FixDist or from the IBM Support Center. For more information on FixDist reference URL: http://aix.boulder.ibm.com/pbin-usa/fixdist.pl/ or send e-mail to aixserv@austin.ibm.com with a subject of "FixDist".

NEC Corporation

OS	Version	Status
EWS-UX/V(Rel4.0)	R1.x - R2.x	not vulnerable
	R3.x - R6.x	vulnerable
EWS-UX/V(Rel4.2)	R7.x - R10.x	vulnerable
EWS-UX/V(Rel4.2MP)	R10.x	vulnerable
UP-UX/V	R2.x	not vulnerable
	R3.x - R4.x	vulnerable
UP-UX/V(Rel4.2MP)	R5.x - R7.x	vulnerable
UX/4800	R11.x	vulnerable

The following is a workaround for 48 series.

ypupdated program is started by the /etc/rc2.d/S75rpc script. First, determine if the server is running, killing it if it is. Then, rename ypupdated so that the /etc/rc2.d/S75rpc script will not find and therefore start it when the system reboots.

```
# uname -a
UNIX_System_V testux 4.2 1 R4000 r4000
# /sbin/ps -ef | /usr/bin/grep ypupdated
    root   359     1  0 08:20:05 ?        0:00
/usr/lib/netsvc/yp/ypupdated
    root 19938   836  0 23:13:20 pts/1    0:00 /usr/bin/grep
ypupdated
# /usr/bin/kill 359
# /sbin/mv /usr/lib/netsvc/yp/ypupdated
/usr/lib/netsvc/yp/ypupdated.CA-95.17
# /usr/bin/chmod 0 /usr/lib/netsvc/yp/ypupdated.CA-95.17
```

Contacts for further information: E-mail:UX48-security-support@nec.co.jp

Open Software Foundation

YP/NIS is not part of the OSF/1 Version 1.3 offering. Hence, OSF/1 Version 1.3 is not vulnerable.

Sequent Computer Systems

Sequent does not support the product referred to in this advisory, and as such is not vulnerable.

Silicon Graphics Inc. (SGI)

IRIX 3.x, 4.x, 5.0.x, 5.1.x, 5.2: vulnerable. Turn off rpc.ypudated in inetd.conf; it is shipped with this turned on.

IRIX 5.3, 6.0, 6.0.1: rpc.ypupdated was off as distributed. Turn off if you have turned it on.

Solbourne

Not vulnerable.

Sun Microsystems, Inc.

BUG 1230027/1232146 fixed in 4.1.3, will not fix 2.4

The ypupdated program is no longer shipped with NS-KIT. If we do decide in the future to support it again, we will fix the bug.

Revision History

Oct. 30, 1997	Updated vendor information for Sun.
Sep. 23, 1997	Updated copyright information
Aug. 30, 1996	Information previously in the README was inserted into the advisory.
Feb. 21, 1996	Appendix, IBM - added an entry for IBM
Dec. 18, 1995	Appendix, Digital & Hewlett-Packard – modified information

18 CA-1995-18: Widespread Attacks on Internet Sites

Original issue date: December 18, 1995
Last revised: September 23, 1997
Updated copyright statement

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

Over the last several weeks, the CERT Coordination Center has been working on a set of incidents in which the intruders have launched widespread attacks against Internet sites. Hundreds of sites have been attacked, and many of the attacks have been successful, resulting in root compromises at the targeted sites. We continue to receive reports, and we believe that more attacks are going undetected.

All the vulnerabilities exploited in these attacks are known, and are addressed by CERT advisories (see Section III).

We urge everyone to obtain these advisories and take action to ensure that systems are protected against these attacks. Also, please feel free to redistribute this message.

We will update this advisory as we receive additional information. Please check advisory files regularly for updates that relate to your site.

Also see CERT Summaries for information on intruder activity:
ftp://ftp.cert.org/pub/cert_summaries/

I. Description

Intruders are doing the following:

- - using automated tools to scan sites for NFS and NIS vulnerabilities
- - exploiting the rpc.ypupdated vulnerability to gain root access
- - exploiting the loadmodule vulnerability to gain root access
- - installing Trojan horse programs and packet sniffers
- - launching IP spoofing attacks

II. Impact

Successful exploitation of the vulnerabilities can result in unauthorized root access.

III. Solution

The CERT staff urges you to immediately take the steps described in the advisories listed below. Note that it is important to check advisories periodically as we add updated information as we receive it.

a. Using automated tools to scan sites for NFS and NIS vulnerabilities

- CA-94.15.NFS.Vulnerabilities
- CA-92.13.SunOS.NIS.vulnerability

b. Exploiting the rpc.ypupdated vulnerability to gain root access

- CA-95.17.rpc.ypupdated.vul

c. Exploiting the loadmodule vulnerability to gain root access

- CA-93.18.SunOS.Solbourne.loadmodule.modload.vulnerability
- A-95.12.sun.loadmodule.vul

d. Installing Trojan horse programs and packet sniffers

- CA-94.01.ongoing.network.monitoring.attacks

e. Launching IP spoofing attacks

- CA-95.01.IP.spoofing

The CERT advisories are available from ftp://ftp.cert.org/pub/cert_advisories.

If you find a compromise, please complete the Incident Reporting Form that we have provided at the end of this advisory, and return the form to cert@cert.org. This completed form will help us better assist you.

Note: Because of our workload, we must ask you not to send log files of activity, but we would be happy to work with you as needed on how to interpret data that you may collect. Also, the CERT staff can provide guidance and advice, if needed, on how to handle incidents and work with law enforcement.

Appendix: Incident Reporting Form

(also available from ftp://ftp.cert.org/pub/incident_reporting_form)

version 3.0

CERT* Coordination Center
Incident Reporting Form

The CERT Coordination Center (CERT/CC) has developed the following form in an effort to gather incident information. We would appreciate your completing the form below in as much detail as possible. The information is optional, but from our experience we have found that having the answers to all the questions enables us to provide the best assistance. Completing the form also helps avoid delays while we get back to you requesting the information we need in order to help you. Sites have told us, as well, that filling out the form has helped them work through the incident.

Note that our policy is to keep any information specific to your site confidential unless we receive your permission to release that information.

Please feel free to duplicate any section as required. Please return this form to cert@cert.org. If you are unable to email this form, please send it by FAX. The CERT/CC FAX number is

+1 412 268 6989

Thank you for your cooperation and help.

```
1.0. General Information
     1.1. Incident number (to be assigned by the CERT/CC):  CERT#
     1.2. Reporting site information
          1.2.1.  Name (e.g., CERT Coordination Center):
          1.2.2.  Domain Name (e.g., cert.org):
          1.2.3.  Brief description of the organization:
          1.2.4.  Is your site an Internet Service Provider (Yes/No):
2.0. Contact Information
     2.1. Your contact information
           2.1.1.  Name:
           2.1.2.  Email address:
           2.1.3.  Telephone number:
           2.1.4.  FAX number:
           2.1.5.  Pager number:
           2.1.6.  Home telephone number (for CERT/CC internal use only):
           2.1.7.  Secure communication channel (e.g., PGP, PEM, DES, secure
                    telephone/FAX) [NOTE -- we will call to obtain the secure
                    communication channel information] (Yes/No):
     2.2. Additional contact information (if available)
           2.2.1.  Name:
           2.2.2.  Email address:
           2.2.3.  Telephone number:
           2.2.4.  FAX number:
           2.2.5.  Pager number:
           2.2.6.  Home telephone number (for CERT/CC internal use only):
           2.2.7.  Secure communication channel (Yes/No):
     2.3. Site security contact information (if applicable)
           2.3.1.  Name:
           2.3.2.  Email address:
           2.3.3.  Telephone number:
           2.3.4.  FAX number:
           2.3.5.  Pager number:
           2.3.6.  Home telephone number (for our internal use only):
           2.3.7.  Secure communication channel (Yes/No):
     2.4. Contact information for other site(s) involved in this incident (if
           available)
           2.4.1.  Site name:
           2.4.2.  Contact person name:
           2.4.3.  Email address:
           2.4.4.  Telephone number:
           2.4.5.  FAX number:
           2.4.6.  Pager number:
           2.4.7.  Home telephone number (for CERT/CC internal use only):
           2.4.8.  Secure communication channel (Yes/No):
```

```
     2.5. Contact information for any other incident response team(s) (IRTs)
           that has/have been notified (if available)
           2.5.1.  IRT name:
           2.5.2.  Constituency domain:
           2.5.3.  Contact person name:
           2.5.4.  Email address:
           2.5.5.  Telephone number:
           2.5.6.  FAX number:
           2.5.7.  Pager number:
           2.5.8.  Home telephone number (for CERT/CC internal use only):
           2.5.9.  Secure communication channel (Yes/No):
           2.5.10. IRT reference number:
     2.6. Contact information for any law enforcement agency(ies) that
          has/have been notified (if available)
          2.6.1.  Law enforcement agency name:
          2.6.2.  Contact person name:
          2.6.3.  Email address:
          2.6.4.  Telephone number:
          2.6.5.  FAX number:
          2.6.6.  Pager number:
          2.6.7.  Home telephone number (for CERT/CC internal use only):
          2.6.8.  Secure communication channel (Yes/No):
          2.6.9.  Law enforcement agency reference number:
3.0. Contacting Sites Involved
     3.1. We ask that reporting sites contact other sites involved in
          incident activity.  Please let us know if you need assistance
          in obtaining contact information for the site(s) involved.
          When contacting the other sites, we would very much
          appreciate a cc to the "cert@cert.org" alias.  This helps
          us identify connections between incidents and understand
          the scope of intruder activity.  We would also appreciate
          your including our incident number in the subject line of
          any correspondence relating to this incident if one
          has been assigned (see item 1.1.).
          If you are unable to contact the involved sites, please get in
          touch with us to discuss how we can assist you.
     3.2. Disclosure information -- may we give the following types of
          information to
          3.2.1. the sites involved in this incident
                 3.2.1.1. your domain (Yes/No):
                 3.2.1.2. your host(s) involved (Yes/No):
                 3.2.1.3. your contact information (Yes/No):
          3.2.2. incident response teams, for sites from their
                 constituencies involved in this incident
                 3.2.2.1. your domain (Yes/No):
                 3.2.2.2. your host(s) involved (Yes/No):
                 3.2.2.3. your contact information (Yes/No):
          3.2.3. law enforcement agency(ies) if there is a legal
                 investigation
                 3.2.3.1. your domain (Yes/No):
                 3.2.3.2. your host(s) involved (Yes/No):
                 3.2.3.3. your contact information (Yes/No):
4.0. Host Information
     4.1. Host(s) involved at your site.  Please provide information on all
          host(s) involved in this incident at the time of the incident (one
          entry per host please)
          4.1.1.  Hostname:
          4.1.2.  IP address(es):
          4.1.3.  Vendor hardware, OS, and version:
          4.1.4.  Security patches applied/installed as currently
                  recommended by the vendor and the CERT/CC
                  (Yes/No/Unknown):
```

```
          4.1.5.  Function(s) of the involved host
                  4.1.5.1. Router (Yes/No):
                  4.1.5.2. Terminal server (Yes/No):
                  4.1.5.3. Other (e.g. mail hub, information server, DNS
                           [external or internal], etc.):
          4.1.6.  Where on the network is the involved host (e.g.
                  backbone, subnet):
          4.1.7.  Nature of the information at risk on the involved host
                  (e.g., router configuration, proprietary, personnel,
                  financial, etc.):
          4.1.8.  Timezone of the involved host (relative to GMT):
          4.1.9.  In the attack, was the host the source, the victim, or
                  both:
          4.1.10. Was this host compromised as a result of this attack
                  (Yes/No):
     4.2. Host(s) involved at other other sites (one entry per host
          please)
          4.2.1. Hostname:
          4.2.2. IP address(es):
          4.2.3. Vendor hardware, OS, and version:
          4.2.4. Has the site been notified (Yes/No):
          4.2.5. In the attack, was the host the source, the victim, or
                 both:
          4.2.6. Was this host compromised as a result of this attack
                 (Yes/No):
5.0. Incident Categories
     5.1. Please mark as many categories as are appropriate to
          this incident
          5.1.1.  Probe(s):
          5.1.2.  Scan(s):
          5.1.3.  Prank:
          5.1.4.  Scam:
          5.1.5.  Email Spoofing:
          5.1.6.  Email bombardment:
                  5.1.6.1. was this denial-of-service attack successful
                           (Yes/No):
          5.1.7.  Sendmail attack:
                  5.1.7.1. did this attack result in a compromise (Yes/No):
          5.1.8.  Break-in
                  5.1.8.1. Intruder gained root access (Yes/No):
                  5.1.8.2. Intruder installed Trojan horse program(s)
                           (Yes/No):
                  5.1.8.3. Intruder installed packet sniffer (Yes/No):
                           5.1.8.3.1. What was the full pathname(s) of the
                                      sniffer output file(s):
                           5.1.8.3.2. How many sessions did the sniffer log?
                                      (use "grep -c 'DATA' <filename>" to
                                      obtain this information):
                  5.1.8.4.  NIS (yellow pages) attack (Yes/No):
                  5.1.8.5.  NFS attack (Yes/No):
                  5.1.8.6.  TFTP attack (Yes/No):
                  5.1.8.7.  FTP attack (Yes/No):
                  5.1.8.8.  Telnet attack (Yes/No):
                  5.1.8.9.  Rlogin or rsh attack (Yes/No):
                  5.1.8.10. Cracked password (Yes/No):
                  5.1.8.11. Easily-guessable password (Yes/No):
          5.1.9.  Anonymous FTP abuse (Yes/No):
          5.1.10. IP spoofing (Yes/No):
          5.1.11. Product vulnerability (Yes/No):
                  5.1.11.1. Vulnerability exploited:
          5.1.12. Configuration error (Yes/No):
                  5.1.12.1. Type of configuration error:
```

```
          5.1.13. Misuse of host(s) resources (Yes/No):
          5.1.14. Worm (Yes/No):
          5.1.15. Virus (Yes/No):
          5.1.16. Other (please specify):
6.0. Security Tools
     6.1. At the time of the incident, were you any using the following
          security tools (Yes/No; How often)
          Network Monitoring tools
             6.1.1.  Argus:
             6.1.2.  netlog (part of the TAMU Security Package):
          Authentication/Password tools
             6.1.3.  Crack:
             6.1.4.  One-time passwords:
             6.1.5.  Proactive password checkers:
             6.1.6.  Shadow passwords:
             6.1.7.  Kerberos:
          Service filtering tools
             6.1.8.  Host access control via modified daemons or wrappers:
             6.1.9.  Drawbridge (part of the TAMU Security Package):
             6.1.10. Firewall (what product):
             6.1.11. TCP access control using packet filtering:
          Tools to scan hosts for known vulnerabilities
             6.1.12. ISS:
             6.1.13. SATAN:
          Multi-purpose tools
             6.1.14. C2 security:
             6.1.15. COPS:
             6.1.16. Tiger (part of the TAMU Security Package):
          File Integrity Checking tools
             6.1.17. MD5:
             6.1.18. Tripwire:
          Other tools
             6.1.19. lsof:
             6.1.20. cpm:
             6.1.21. smrsh:
             6.1.22. append-only file systems:
          Additional tools (please specify):
     6.2. At the time of the incident, which of the following logs were you
          using, if any (Yes/No)
          6.2.1. syslog:
          6.2.2. utmp:
          6.2.3. wtmp:
          6.2.4. TCP wrapper:
          6.2.5. process accounting:
     6.3. What do you believe to be the reliability and integrity of
          these logs (e.g., are the logs stored offline or on a
          different host):
7.0. Detailed description of the incident
     7.1. Please complete in as much detail as possible
          7.1.1.  Date and duration of incident:
          7.1.2.  How you discovered the incident:
          7.1.3.  Method used to gain access to the affected host(s):
          7.1.4.  Details of vulnerabilities exploited that are
                  not addressed in previous sections:
          7.1.5.  Other aspects of the "attack":
          7.1.6.  Hidden files/directories:
          7.1.7.  The source of the attack (if known):
          7.1.8.  Steps taken to address the incident (e.g., binaries
                  reinstalled, patches applied):
          7.1.9.  Planned steps to address the incident (if any):
          7.1.10. Do you plan to start using any of the tools listed
                  above in question 6.0 (please list tools expected
                  to use):
          7.1.11. Other:
     7.2. Please append any log information or directory listings and
          timezone information (relative to GMT).
     7.3. Please indicate if any of the following were left on your
          system by the intruder (Yes/No):
          7.3.1. intruder tool output (such as packet sniffer output
                 logs):
          7.3.2. tools/scripts to exploit vulnerabilities:
          7.3.3. source code programs (such as Trojan horse programs,
                 sniffer programs):
          7.3.4. binary code programs (such as Trojan horse programs,
                 sniffer programs):
          7.3.5. other files:
          If you answered yes to any of the last 5 questions, please call
          the CERT/CC hotline (+1 412 268 7090) for instructions on
          uploading files to us by FTP.  Thanks.
     7.4. What assistance would you like from the CERT/CC?
```

Revision History

Sep. 23, 1997 Updated copyright statement

Aug. 30, 1996 - Removed references to README files because updated information is put into the advisories themselves.

Added a pointer to CERT summaries.

Updated the file name for the incident reporting form (IRF).

Replaced the old version of the IRF with version 3.0.