1 CA-1996-01: UDP Port Denial-of-Service Attack

Original issue date: February 8, 1996
Last revised: September 24, 1997
Updated copyright statement

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

The CERT Coordination Center has received reports of programs that launch denial-of-service attacks by creating a "UDP packet storm" either on a system or between two systems. An attack on one host causes that host to perform poorly. An attack between two hnosts can cause extreme network congestion in addition to adversely affecting host performance.

The CERT staff recommends disabling unneeded UDP services on each host, in particular the chargen and echo services, and filtering these services at the firewall or Internet gateway.

Because the UDP port denial-of-service attacks typically involve IP spoofing, we encourage you to follow the recommendations in advisory CA-96.21.

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

I. Description

When a connection is established between two UDP services, each of which produces output, these two services can produce a very high number of packets that can lead to a denial of service on the machine(s) where the services are offered. Anyone with network connectivity can launch an attack; no account access is needed.

For example, by connecting a host's chargen service to the echo service on the same or another machine, all affected machines may be effectively taken out of service because of the excessively high number of packets produced. In addition, if two or more hosts are so connected, the intervening network may also become congested and deny service to all hosts whose traffic traverses that network.

II. Impact

Anyone with network connectivity can cause a denial of service. This attack does not enable them to gain additional access.

III. Solution

We recommend taking all the steps described below.

1. Disable and filter chargen and echo services.

This attack is most readily exploited using the chargen or echo services, neither of which is generally needed as far as we are aware. We recommend that you disable both services on the host and filter them at the firewall or Internet gateway.

To disable these services on a host, it is necessary to edit the inetd configuration file and cause inetd to begin using the new configuration. Exactly how to do this is system dependent so you should check your vendor's documentation for *inetd(8)*; but on many UNIX systems the steps will be as follows:

1. Edit the inetd configuration file (e.g. /etc/inetd.conf).
2. Comment out the echo, chargen, and other UDP services not used.
3. Cause the inetd process to reread the configuration file (e.g., by sending it a HUP signal).

2. Disable and filter other unused UDP services.

To protect against similar attacks against other services, we recommend:

- disabling all unused UDP services on hosts and
- blocking at firewalls all UDP ports less than 900 with the exception of specific services you require, such as DNS (port 53).

3. If you must provide external access to some UDP services, consider using a proxy mechanism to protect that service from misuse.

Techniques to do this are discussed in Chapter 8, "Configuring Internet Services," in _Building Internet Firewalls_ by Chapman and Zwicky (see Section IV below).

4. Monitor your network.

If you do provide external UDP services, we recommend monitoring your network to learn which systems are using these services and to monitor for signs of misuse. Tools for doing so include Argus, tcpdump, and netlog.

Argus is available from

ftp://ftp.net.cmu.edu/pub/argus-1.5/
MD5 (argus-1.5.tar.gz) = 9c7052fb1742f9f6232a890267c03f3c

Note that Argus requires the TCP wrappers to install:

ftp://ftp.cert.org/pub/tools/tcp_wrappers/tcp_wrappers_7.2.tar.Z
MD5 (tcp_wrappers_7.2.tar.Z) = 883d00cbd2dedd9bfc783b7065740e74

tcpdump is available from

ftp://ftp.ee.lbl.gov/tcpdump-3.0.2.tar.Z
MD5 (tcpdump-3.0.2.tar.Z) = c757608d5823aa68e4061ebd4753e591

Note that tcpdump requires libpcap, available at ftp://ftp.ee.lbl.gov/libpcap-0.0.6.tar.Z
MD5 (libpcap-0.0.6.tar.Z) = cda0980f786932a7e2eebfb2641aa7a0

netlog is available from ftp://net.tamu.edu/pub/security/TAMU/netlog-1.2.tar.gz
MD5 (netlog-1.2.tar.gz) = 1dd62e7e96192456e8c75047c38e994b

5. Take steps against IP spoofing.

Because IP spoofing is typically involved in UDP port denial-of-service attacks, we encourage you to follow the guidance in advisory CA-95:01, available from www.cert.org/advisories/CA-95.01.IP.spoofing.html.

IV. Sources of further information about packet filtering

For a general packet-filtering recommendations, see ftp://ftp.cert.org/pub/tech_tips/packet_filtering.

For in-depth discussions of how to configure your firewall, see

Firewalls and Internet Security: Repelling the Wily Hacker
William R. Cheswick and Steven M. Bellovin
Addison-Wesley Publishing Company, 1994
ISBN 0-201-63357

Building Internet Firewalls
Brent Chapman and Elizabeth D. Zwicky
O'Reilly & Associates, Inc., 1995
ISBN 1-56592-124-0

The CERT Coordination Center staff thanks Peter D. Skopp of Columbia University for reporting the vulnerability and Steve Bellovin of AT&T Bell Labs for his support in responding to this problem.

UPDATES

Cisco

Cisco Alert Summary: http://www.cisco.com/warp/public/146/917_security.html

Cisco Security Guide: http://www.cisco.com/univercd/data/doc/cintrnet/ics/icssecur.htm

Silicon Graphics Inc.

SGI acknowledges CERT Advisory CA-96.01 and is currently investigating. No further information is available at this time.

Revision History

Sep. 24, 1997 Updated copyright statement

Feb. 14, 1997 Introduction - updated the IP spoofing reference to CA-96.21.

Updates section - added pointers to CISCO documents.

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

Feb. 23, 1996 Updates section - added information from Silicon Graphics, Inc.

Feb. 21, 1996 Solution, Sec. III.4 - added new URL for Argus.

2 CA-1996-02: BIND Version 4.9.3

CERT(sm) Advisory CA-96.02
Original issue date: February 15, 1996
Last revised: August 13, 1997
Superseded by CA-97.22
A complete revision history is at the end of this advisory.
Topic: BIND Version 4.9.3

** This advisory has been superseded by CA-97.22.bind **
Vulnerabilities in the Berkeley Internet Name Domain (BIND) program make it possible for intruders to render Domain Name System (DNS) information unreliable. At the beginning of this year, a version of BIND (4.9.3) became available that fixes several security problems that are being exploited by the intruder community. The CERT staff urges you to install the appropriate patch from your vendor. If a patch is not currently available, an alternative is to install BIND 4.9.3 yourself. (Note: Although BIND will be further improved in the future, we urge you to upgrade now because of the seriousness of the problems addressed by version 4.9.3.) If neither of the above alternatives is possible, we strongly recommend blocking or turning off DNS name-based authentication services such as rlogin. We will update this advisory as we receive additional information. Please check advisory files regularly for updates that relate to your site.

I. Description
Version 4.9.3 of the Berkeley Internet Name Domain (BIND) program fixes several security problems that are well known and being exploited by the intruder community to render Domain Name System (DNS) information unreliable. BIND is an implementation of the Domain Name System. (For details, see RFC 1035, a publication of the Internet Engineering Task Force.) The full distribution of BIND includes a number of programs and resolver library routines. The main program is "named", the daemon that provides DNS information from local configuration files and a local cache. The named daemon is often called /etc/named or /etc/in.named. Programs such as Telnet communicate with named via the resolver library routines provided in the BIND distribution. Services in widespread use that depend on DNS information for authentication include rlogin, rsh (rcp), xhost, and NFS. Sites may have installed locally other services that trust DNS information. In addition, many other services, such as Telnet, FTP, and email, trust DNS information. If these services are used only to

make outbound connections or informational logs about the source of connections, the security impact is less severe than for services such as rlogin. Although you might be willing to accept the risks associated with using these services for now, you need to consider the impact that spoofed DNS information may have. Although the new BIND distributions do address important security problems, not all known problems are fixed. In particular, several problems can be fixed only with the use of cryptographic authentication techniques. Implementing and deploying this solution is non-trivial; work on this task is currently underway within the Internet community. The CERT staff has received information that the next minor release of BIND nameserver will be enforcing RFC952 (as modified by RFC1123) hostname conformance as part of its SECURITY measures. Following The BIND release, hostnames that fail to conform to these rules will be unreachable from sites running these servers. Hostnames (A records) are restricted to the following characters only:

"A" - "Z", "a" - "z", "0" - "9", "." and "-"

These characters are specifically excluded: "_" and "/". For a full description of what is allowed in a hostname, please refer to RFC952 and RFC1123, available from http://ds.internic.net/ds/

RFC952: DOD INTERNET HOST TABLE SPECIFICATION, October 1985

RFC1123: Requirements for Internet Hosts -- Application and Support, October 1989

A program is available for checking hostnames and IP addresses. It is available in

ftp://info.cert.org/pub/tools/ValidateHostname/IsValid.c

ftp://ftp.cert.dfn.de/pub/tools/net/ValidateHostname/IsValid.c

The following files are in the directory (from the README):

IsValid.l — The lex/flex file containing the code for IsValidHostname and IsValidIPAddress
MD5 (IsValid.l) = 2d35040aacae4fb12906eb1b48957776

IsValid-raw.c — The C file created by running flex on IsValid.l
MD5 (IsValid-raw.c) = 367c77d3ef84bc63a5c23d90eeb69330

IsValid.c — The editted file created by internalizing variable and function definitions in IsValid-raw.c
MD5 (IsValid.c) = ffe45f1256210aeb71691f4f7cdad27f

IsValid.diffs — The set of diffs between IsValid-raw.c and IsValid.c
MD5 (IsValid.diffs) = 3619022cf31d735151f8e8c83cce3744

htest.c — A main routing for testing IsValidHostname and IsValidIPAddress

MD5 (htest.c) = 2d50b2bffb537cc4e637dd1f07a187f4

II. Impact
It is possible for intruders to spoof BIND into providing incorrect name data. Some systems and programs depend on this information for authentication, so it is possible to spoof those systems and gain unauthorized access.

III. Solutions The preferred solution, described in Section A, is to install your vendor's patch if one is available. An alternative (Section B) is to install the latest version of BIND. In both cases, we encourage you to take the additional precautions described in Section C.

A. Obtain the appropriate patch from your vendor and install it according to instructions included with the program. Redistributing BIND and all programs affected by these problems is not a simple matter, so some vendors are working on new named daemon as an immediate patch. Although installing a new named daemon addresses some problems, significant problems remain that can be addressed only by fully installing fixes to the library resolver routines. If your vendor's patch does not include both named and new resolver routines, we recommend that you install the current version of BIND (Solution B) if possible. We also encourage you to take the precautions described in Section C. Below is a list of the vendors and the status they have provided concerning BIND. More complete information is provided in Appendix A of this advisory. We will update the appendix as we receive more information from vendors. If your vendor's name is not on the list, contact the vendor directly for status information and further instructions.

Vendor	New named available	Full distribution available
Digital Equipment		Work is under way.
Hewlett-Packard	Under investigation.	Currently porting and testing
		(BIND 4.9.3) for the Q1, Calendar 97
		general release. Patch in process
		for 10.X releases.
IBM Corporation		Work is under way.
NEC Corporation		Work is under way.
Santa Cruz Operation		Under consideration.
Silicon Graphics, Inc.		Under investigation.
Solbourne (Grumman)		Customers should install BIND 4.9.3.
Sun Microsystems		Patches available.

B. Install the latest version of BIND (version 4.9.3), available from Paul Vixie, the current maintainer of BIND:

ftp://ftp.vix.com/pub/bind/release/4.9.3/bind-4.9.3-REL.tar.gz

MD5 (bind-4.9.3-REL.tar.gz) = da1908b001f8e6dc93fe02589b989ef1

Also get Patch #1 for 4.9.3:

ftp://ftp.vix.com/pub/bind/release/4.9.3/Patch1

MD5 (Patch1) = 5d57ad13381e242cb08b5da0e1e9c5b9

To find the most current version of bind, see ftp://info.cert.org/pub/latest_sw_versions/

C. Take additional precautions.

To protect against vulnerabilities that have not yet been addressed, and as good security practice in general, filter at a router all name-based authentication services so that you do not rely on DNS information for authentication. This includes the services rlogin, rsh (rcp), xhost, NFS, and any other locally installed services that provide trust based on domain name information.

.....

Appendix A

Below is information we have received from vendors. If you do not see an entry for your vendor, please contact the vendor directly for status information and further instructions.

- ----------

Paul Vixie

See Updates Section

- ----------

Digital Equipment Corporation

At the time of writing this advisory, Digital intends to support the final revision of BIND 4.9.3. The project plan for incorporating Version 4.9.3 BIND for Digital's ULTRIX platforms has been approved. This includes 4.3, V4.3A, V4.4 and V4.5. A similar project plan for Digital UNIX versions is under review. The first implementations will be V3.0 through V3.2D, and V4.0, when released. It is our plan to evaluate and then incorporate V4.9.3 Bind into other UNIX versions as necessary to reduce risk to our customer base. Digital will provide notice of the completion of the kits through AES services (DIA, DSNlink FLASH) and be available from your normal Digital Support channel.

- ----------

Hewlett-Packard Company

The named daemon is under investigation. HP will provide updated information for the CERT advisory. HP is currently porting and testing BIND 4.9.3 for a general release first quarter of 1997. A patch

```
is in process for 10.X releases. Watch for CERT advisory updates and
a Security Bulletin from HP.
- ------------------------------------
IBM Corporation
Work is under way.
- ------------------------------------
NEC Corporation
Some systems are vulnerable. We are developing the patches and plan
to put them on our anonymous FTP server. You can contact us with the
following e-mail address if you need.
E-mail: UX48-security-support@nec.co.jp
FTP server: ftp://ftp.meshnet.or.jp
- ------------------------------------
The Santa Cruz Operation, Inc.
SCO is currently considering a port of the new BIND into its product
line, but no timeline is yet available. This includes SCO OpenServer
and SCO UNIXWare.
- ------------------------------------
Silicon Graphics Inc.
SGI acknowledges CERT Advisory CA-96.02 and is currently investigat-
ing.
No further information is available at this time.
As further information becomes available, additional advisories will
be available from ftp://sgigate.sgi.com.
- ------------------------------------
Solbourne (Grumman)
Solbourne have determined that Solbourne Computers are vulnerable A
patch is not available and they recommend Solbourne customers in-
stall
BIND version 4.9.3.
- ------------------------------------
Sun Microsystems, Inc.
Sun Security Patches and Bulletins are available through your local
SunService and SunSoft Support Services organizations, via the secu-
rity-alert alias (security-alert@sun.com) and on SunSolve Online:
        http://sunsolve1.sun.com/
SunOS 5.3/Solaris 2.3
- --------------------
        101359-03       SunOS 5.3: DNS spoofing is possible per CERT
CA-96.02
        101739-12       sendmail patch
        102167-03       nss_dns.so.1 rebuild for BIND 4.9.3
        103705-01       rpc.nisd_resolv rebuild for BIND 4.9.3
SunOS 5.4/Solaris 2.4
- --------------------
```

```
        102479-02       SunOS 5.4: DNS spoofing is possible per CERT
CA-96.02
        102066-11       sendmail patch
        102165-03       nss_dns.so.1 rebuild for BIND 4.9.3
        103706-01       rpc.nisd_resolv rebuild for BIND 4.9.3
SunOS 5.4_x86/Solaris 2.4_x86
- ----------------------------
        102480-02       SunOS 5.4_x86: DNS spoofing is possible per
                          CERT CA-96.02
        102064-10       sendmail patch
        102166-03       nss_dns.so.1 rebuild for BIND 4.9.3
        103707-01       rpc.nisd_resolv rebuild for BIND 4.9.3
SunOS 5.5/Solaris 2.5
- --------------------
        103667-01       SunOS 5.5: DNS spoofing is possible per CERT
CA-96.02
        102980-07       sendmail patch
        103279-02       nscd/nscd_nischeck rebuild for BIND 4.9.3
        103703-01       nss_dns.so.1 rebuild for BIND 4.9.3
        103708-01       rpc.nisd_resolv rebuild for BIND 4.9.3
SunOS 5.5_x86/Solaris 2.5_x86
- ----------------------------
        103668-01       SunOS 5.5_x86: DNS spoofing is possible per
                          CERT CA-96.02
        102981-07       sendmail patch
        103280-02       nscd/nscd_nischeck rebuild for BIND 4.9.3
        103704-01       nss_dns.so.1 rebuild for BIND 4.9.3
        103709-01       rpc.nisd_resolv rebuild for BIND 4.9.3
SunOS 5.5.1/Solaris 2.5.1
- ------------------------
        103663-01       SunOS 5.5.1: DNS spoofing is possible per
CERT CA-96.02
        103594-03       sendmail patch
        103680-01       nscd/nscd_nischeck rebuild for BIND 4.9.3
        103683-01       nss_dns.so.1 rebuild for BIND 4.9.3
        103686-01       rpc.nisd_resolv rebuild for BIND 4.9.3
SunOS 5.5.1_ppc/Solaris 2.5.1_ppc
- --------------------------------
        103665-01       SunOS 5.5.1_ppc: DNS spoofing is possible
                        Per CERT CA-96.02
        103596-03       sendmail patch
        103682-01       nscd/nscd_nischeck rebuild for BIND 4.9.3
        103685-01       nss_dns.so.1 rebuild for BIND 4.9.3
        103688-01       rpc.nisd_resolv rebuild for BIND 4.9.3
SunOS 5.5.1_x86/Solaris 2.5.1_x86
- --------------------------------
```

```
        103664-01       SunOS 5.5.1_x86: DNS spoofing is possible
                        Per CERT CA-96.02
        103595-03       sendmail patch
        103681-01       nscd/nscd_nischeck rebuild for BIND 4.9.3
        103684-01       nss_dns.so.1 rebuild for BIND 4.9.3
        103687-01       rpc.nisd_resolv rebuild for BIND 4.9.3
- -----------------------------------------------------------------
```

The CERT Coordination Center wishes to thank Paul Vixie for his efforts in responding to this problem and his aid in developing this advisory.

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

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). We strongly urge you to encrypt any sensitive information you send by email. The CERT Coordination Center can support a shared DES key and PGP. Contact the CERT staff for more information.

Location of CERT PGP key
ftp://info.cert.org/pub/CERT_PGP.key

CERT Contact Information
- ------------------------

Email cert@cert.org
Phone +1 412-268-7090 (24-hour hotline)
CERT personnel answer 8:30-5:00 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

To be added to our mailing list for CERT advisories and bulletins, send your email address to cert-advisory-request@cert.org

CERT publications, information about FIRST representatives, and other security-related information are available for anonymous FTP from ftp://info.cert.org/pub/
CERT advisories and bulletins are also posted on the USENET newsgroup comp.security.announce

==========

UPDATES
June 25, 1997
- ------------

If you are running BIND 8.1 you want to upgrade. The current version of BIND (8.8.1) is available by anonymous FTP from
  ftp://ftp.isc.org/isc/bind/src/8.1.1
If you are still running BIND-4 rather than BIND-8, you need the security patches contained in BIND 4.9.6. Available from
ftp://ftp.isc.org/isc/bind/src/4.9.6/
The author of BIND encourages sites to switch to BIND-8.

~~~~~~~~~~

Revision History
Aug. 13, 1997 This advisory superseded by CA-97.22.
June 25, 1997 Appendix, Changed Vixie entry to point to Updates.
               Updates section - Current release information.
May 22, 1997 Updates section - noted current version of BIND and new location for the BIND archives.
Aug. 30, 1996 Information previously in the README was inserted into the advisory.
Aug. 01, 1996 Appendix - updated Sun patch information
Apr. 08, 1996 Sec. I - added information about the next release of BIND and the IsValid program to the end of the section
Mar. 29, 1996 Appendix, Sun - added information
Feb. 27, 1996 Appendix, SGI - added an entry
Feb. 21, 1996 Appendix, IBM & Solbourne - added entries
~~~~~~~~~~

3 CA-1996-03: Vulnerability in Kerberos 4 Key Server

Original issue date: February 21, 1996
Last revised: September 24, 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 the Kerberos Version 4 server. On unpatched Kerberos 4 systems, under certain circumstances, intruders can masquerade as authorized Kerberos users and gain access to services and resources not intended for their use. The CERT team recommends that you apply one of the solutions given in Section III.

The Kerberos Version 5 server running in Version 4 compatibility mode is also vulnerable under certain circumstances. The Massachusetts Institute of Technology (MIT) is working on the patches for that version.

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 Kerberos Version 4 server is using a weak random number generator to produce session keys. On a computer of average speed, the session key for a ticket can be broken in a maximum of 2-4 minutes, and sometimes in much less time. This means that usable session keys can be manufactured without a user first being authorized by Kerberos.

II. Impact

Under certain circumstances, intruders can masquerade as authorized Kerberos users and gain access to services and resources not intended for their use.

III. Solution

If you are running Kerberos Version 4 and have built Kerberos from a source distribution, use solution A. If you have obtained Kerberos 4 binaries from a vendor, use solution B. If you are now using Kerberos Version 5, be aware that MIT is working on patches for that version. Notice will be made when the patches are available.

A. Solution for Source Distributions

If you have built Kerberos Version 4 from source, follow these instructions to retrieve the fixes necessary to correct this problem:

Use anonymous FTP to athena-dist.mit.edu. Change directory to /pub/kerberos, fetch and read "README.KRB4" found in that directory. It will provide the name of the distribution directory (which is otherwise hidden and cannot be found by listing its parent directory). Change directory to the hidden distribution directory. There you will find the original Kerberos distribution plus a new file named "random_patch.tar.Z" (and random_patch.tar.gz for those with "gzip"). This tar file contains two files, the patch itself and a README.PATCH file. Read this file carefully before proceeding.

As of February 23, 1996, MIT has updated the patch described in advisory CA-96.03. The actual patch has not changed, but the README.PATCH file (part of random_patch.tar.*) which contains instructions on how to install the patch has been edited to include the following new paragraph:

IMPORTANT: After running fix_kdb_keys you must kill and restart the kerberos server process (it has the old keys cached in memory). Also, if you operate any Kerberos slave servers, you need to perform a slave propagation immediately to update the keys on the slaves.

Updated files are now available on "athena-dist.mit.edu" including an updated random_patch.md5 file which contains the MD5 checksums of random_patch.tar.* The PGP Signature is issued by Jeffrey I. Schiller <jis@mit.edu> using PGP keyid 0x0DBF906D. The fingerprint is

DD DC 88 AA 92 DC DD D5 BA 0A 6B 59 C1 65 AD 01

The updated files are also available from
ftp://ftp.cert.org/pub/vendors/mit/Patches/Kerberos-V4/.

The new checksums are

MD5 (random_patch.md5) = ecf5412094572e183aa33ae4e5f197b8
MD5 (random_patch.tar.Z) = e925b687a05a8c6321b2805026253315
MD5 (random_patch.tar.gz) = 003226914427094a642fd1f067f589d2

These files are also available from

ftp://ftp.cert.org/pub/vendors/mit/Patches/Kerberos-V4/random_patch.md5

ftp://ftp.cert.org/pub/vendors/mit/Patches/Kerberos-V4/random_patch.tar.Z

ftp://ftp.cert.org/pub/vendors/mit/Patches/Kerberos-V4/random_patch.tar.gz

The checksums are the same as above.

B. Solution for Binary Distributions

Contact your vendor.

Some vendors who provide Kerberos are sending the CERT Coordination Center information about their patches. Thus far, we have received information from one vendor and placed it in the appendix of this advisory. We will update the appendix as we hear from vendors.

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.

The Santa Cruz Operation, Inc.

The Kerberos 4 problem does not affect SCO.

SCO OpenServer, SCO Open Desktop, SCO UnixWare, SCO Unix, and SCO Xenix do not support Kerberos.

The SCO Security Server, an add-on product for SCO OpenServer 3 and SCO OpenServer 5, supports Kerberos V5 authentication. This product cannot be configured to be Kerberos V4 compatible; therefore, it is not vulnerable.

TGV Software, Inc.

TGV has made two Kerberos ECO kits available (one for MultiNet V3.4 and one for V3.5) for Anonymous FTP. If you are running Kerberos, we _strongly_ urge you to apply this kit.

To obtain the kit, FTP to ECO.TGV.COM, username ANONYMOUS, password either KERBEROS-034 or KERBEROS-035 (depending on the version of MultiNet that you are running) and download the ECO kit: ftp://anonymous:kerberos-035@eco.tgv.com.

The kit is available in both VMS BACKUP save set format as well as in a compressed .ZIP file. Use VMSINSTAL to apply the ECO.

Once you have completed the upgrade, the KITREMARK.VUR file from the ECO kit will be displayed providing instructions during the installation process.

If you have any questions, please send an e-mail message to MultiNet-VMS@Support.TGV.COM.

Transarc Corporation

Kerberos Version 4.0 is used in our AFS product (all versions of AFS), while Kerberos Version 5.0 is used in our DCE product (Kerberos Version 5.0 is used in ALL DCE products).

In light of the COAST work, Transarc is doing a security review of Kerberos 4.0 and AFS. We expect to provide some procedural changes to improve security in new cells, and we will make code changes as necessary. OSF also reviewed Kerberos 5.0, and they have released a source patch for Kerberos 5.0 that strengthens the random number generator in Kerberos 5.0. This patch is relevant to all versions of DCE (but not to AFS since it is based on Kerberos 4.0).

Transarc has this OSF patch available for DCE 1.1 on Solaris 2.4, DCE 1.0.3a on Solaris 2.4, DCE 1.0.3a on Solaris 2.3, and DCE 1.0.3a on Sun OS 4.1.3. Please contact Transarc Customer Support for access to these patches.

Please feel free to contact me directly if you have further questions about this issue.

For pointers and background on these issues please refer to
http://www.transarc.com/afs/transarc.com/public/www/Public/Support/security-\ update.html.

Liz Hines
Hines@transarc.com

The CERT Coordination Center thanks Jeffrey Schiller and Theodore Ts'o of Massachusetts Institute of Technology for their effort in responding to this problem, and thanks Gene Spafford of COAST for the initial information about the problem.

Revision History

Sep. 24, 1997 Updated copyright statement

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

Mar. 08, 1996 Appendix, TGV Software & Transarc - added entries

Feb. 23, 1996 Sec. III.A - noted a change in the readme.patch file and put new MD5 checksums at the end of the section.

4 CA-1996-04: Corrupt Information from Network Servers

Original issue date: February 22, 1996
Last revised: April 28, 1998
Corrected URL for obtaining RFCs. Removed obsolete references to a latest_sw_versions directory.

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

The CERT Coordination Center has received reports of intruders exploiting systems by corrupting data provided by a Domain Name Service (DNS) server. Although these reports have focused only on DNS, this vulnerability could apply to any network service from which data is received and subsequently used.

Section III.A contains a pointer to two subroutines that address the DNS problem. These subroutines, written in the C programming language, can be used to validate host names and IP addresses according to RFCs 952 and 1123, as well as names containing characters drawn from common practice, namely "_" and "/".

In the specific case of sendmail, the problem has already been addressed by patches (see Section III.B).

The CERT staff has received information that the next minor release of BIND nameserver will be enforcing RFC952 (as modified by RFC1123) hostname conformance as part of its SECURITY measures. Following The BIND release, hostnames that fail to conform to these rules will be unreachable from sites running these servers.

Hostnames (A records) are restricted to the following characters only:

"A" - "Z", "a" - "z", "0" - "9", "." and "-"

These characters are specifically excluded: "_" and "/".

For a full description of what is allowed in a hostname, please refer to RFC952 and RFC1123, available from

ftp://ftp.isi.edu/in-notes/rfc952.txt

ftp://ftp.isi.edu/in-notes/rfc1123.txt

RFC952: DOD INTERNET HOST TABLE SPECIFICATION, October 1985
RFC1123: Requirements for Internet Hosts -- Application and Support, October 1989

The latest release of Bind is available from: ftp://ftp.isc.org/isc/bind/src/.

I. Description

Information provided by an information server may be of a form that could cause programs to operate in unexpected ways. The subroutines and programs transferring data from that information server could check the data for correctness of form; however, programs that *use* that data are ultimately responsible for ensuring adherence to the documents that define the correct form.

For example, consider a program that uses the host name returned by gethostbyname() as part of the string given to the popen() or system() subroutines. Because gethostbyname() may use an information server beyond your control, the data returned could be of a form that causes the popen() or system() subroutines to execute other commands besides the command specified by that program.

This advisory speaks to a specific instance of a problem caused by the information returned by DNS, but information from any server should be checked for validity. Examples of other information servers are YP, NIS, NIS+, and netinfo.

II. Impact

Programs that do not check data provided by information servers may operate in unpredictable ways and give unexpected results. In particular, exploitation of this vulnerability may allow remote access by unauthorized users. Exploitation can also lead to root access by both local and remote users.

III. Solution

For programs that you write or have written, consider integrating the general solution in Section A below.

In the specific case of the sendmail mail delivery program, Eric Allman, the original author of sendmail, has produced patches that address the problem. Section B provides details about these, along with vendor information and additional steps you should take to protect sendmail.

A. General solution for Internet host names

Use the host name and IP address validation subroutines available at the locations listed below. Include them in all programs that use the result of the host name lookups in any way.

ftp://ftp.cert.org/pub/tools/ValidateHostname/IsValid.c

ftp://ftp.cert.dfn.de/pub/tools/net/ValidateHostname/IsValid.c

The IsValid.c file contains code for the IsValidHostname and IsValidIPAddress subroutines. This code can be used to check host names and IP addresses for validity according to RFCs 952 and 1123, well as names containing characters drawn from common practice, namely "_" and "/".

The following files are in the directory (from the README):

IsValid.l	The lex/flex file containing the code for IsValidHostname and IsValidIPAddress MD5 (IsValid.l) = 2d35040aacae4fb12906eb1b48957776
IsValid-raw.c	The C file created by running flex on IsValid.l MD5 (IsValid-raw.c) = 367c77d3ef84bc63a5c23d90eeb69330
IsValid.c	The editted file created by internalizing variable and function definitions in IsValid-raw.c MD5 (IsValid.c) = ffe45f1256210aeb71691f4f7cdad27f
IsValid.diffs	The set of diffs between IsValid-raw.c and IsValid.c MD5 (IsValid.diffs) = 3619022cf31d735151f8e8c83cce3744
htest.c	A main routing for testing IsValidHostname and IsValidIPAddress MD5 (htest.c) = 2d50b2bffb537cc4e637dd1f07a187f4

B. Specific solutions in the case of sendmail

Install a patch from your vendor when it becomes available (see B.1) or install Eric Allman's patch (B.2). In both cases, install the sendmail restricted shell program (B.3).

1. Install a patch from your vendor.

Below is a summary of the vendors who have reported status to us as of the date of this advisory. More complete information is provided in the appendix, which we will update as we receive more information.

If your vendor's name is not on this list, please contact the vendor directly.

Vendor or Source

Eric Allman
Hewlett-Packard Co.
IBM Corporation
Silicon Graphics Inc.
Sun Microsystems, Inc.

2. Install a patch to sendmail.

If you are presently running sendmail 8.6.12, there is a patch that makes version 8.6.13.

Similarly, if you are presently running sendmail 8.7.3, there is a patch that makes version 8.7.4.

The patches are available for anonymous FTP from

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

ftp://ftp.cs.berkeley.edu/ucb/src/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 the 8.6.13 release:

MD5 (sendmail.8.6.13.base.tar.Z) = e8cf3ea19876d9b9def5c0bcb793d241
MD5 (sendmail.8.6.13.cf.tar.Z) = 4492026fa9e750cd33974322cb5a6fb9
MD5 (sendmail.8.6.13.misc.tar.Z) = 7ec5d31656e93e08a3892f0ae542b674
MD5 (sendmail.8.6.13.xdoc.tar.Z) = e4d3caebcdc4912ed2ecce1a77e45712

Checksum for the 8.6.13 patch:

MD5 (sendmail.8.6.13.patch) = 6390b792cb5513ff622da8791d6d2073

Checksum for the 8.7.4 release:

MD5 (sendmail.8.7.4.tar.Z) = 4bf774a12752497527aae11e2bdbab36

Checksum for the 8.7.4 patch:

MD5 (sendmail.8.7.4.patch) = ef828ad91fe56e4eb6b0cacced864cd5

3. Run smrsh as additional protection for sendmail.

With all versions of sendmail, we recommend that you install and use the sendmail restricted shell program (smrsh). We urge you to do this whether you use the vendor's supplied sendmail, install sendmail yourself, or patch an earlier version of sendmail.

Beginning with version 8.7.1, smrsh is included in the sendmail distribution, in the subdirectory smrsh. See the RELEASE_NOTES file for a description of how to integrate smrsh into your sendmail configuration file.

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.

Eric Allman (original author of sendmail)

Install a patch to sendmail.

If you are presently running sendmail 8.6.12, there is a patch that makes version 8.6.13.

Similarly, if you are presently running sendmail 8.7.3, there is a patch that makes version 8.7.4.

The patches are available for anonymous FTP from

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

ftp://ftp.cs.berkeley.edu/ucb/src/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 the 8.6.13 release:

MD5 (sendmail.8.6.13.base.tar.Z) = e8cf3ea19876d9b9def5c0bcb793d241
MD5 (sendmail.8.6.13.cf.tar.Z) = 4492026fa9e750cd33974322cb5a6fb9
MD5 (sendmail.8.6.13.misc.tar.Z) = 7ec5d31656e93e08a3892f0ae542b67
MD5(sendmail.8.6.13.xdoc.tar.Z) = e4d3caebcdc4912ed2ecce1a77e45712

Checksum for the 8.6.13 patch:

MD5 (sendmail.8.6.13.patch) = 6390b792cb5513ff622da8791d6d2073

Checksum for the 8.7.4 release:

MD5 (sendmail.8.7.4.tar.Z) = 4bf774a12752497527aae11e2bdbab36

Checksum for the 8.7.4 patch:

MD5 (sendmail.8.7.4.patch) = ef828ad91fe56e4eb6b0cacced864cd5

Hewlett-Packard Company

Vulnerable, watch file for updates.

IBM Corporation

IBM is working on fixes for sendmail.

Silicon Graphics Inc.

It is **HIGHLY RECOMMENDED** that these measures be done on ALL SGI systems running IRIX 3.x, 4.x, 5.x and 6.x. The issue will be permanently corrected in a future release of IRIX.

**** IRIX 3.x ****

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 patch or
2) obtain the sendmail source code from anonymous FTP at ftp.cs.berkeley.edu and compile the program manually. Please, note that SGI will not assist with or support 3rd party sendmail programs.

**** IRIX 4.x ****

As of the date of this document, SGI does not have a IRIX 4.x binary replacement that addresses this particular issue. If in the future, a replacement binary is generated, additional advisory information will be provided.

However, two other possible actions are:
1) upgrade the system to a supported version of IRIX (see below) and then install the patch or
2) obtain the sendmail source code from anonymous FTP at **Error! Hyperlink reference not valid.** and compile the program manually. Please, note that SGI will not assist with or support 3rd party sendmail programs.

**** IRIX 5.0.x, 5.1.x ****

For the IRIX operating systems versions 5.0.x and 5.1.x, an upgrade to 5.2 or better is required first. When the upgrade is completed, then the patches described in the following sections can be applied depending on the final version of the upgrade.

**** IRIX 5.2, 5.3, 6.0, 6.0.1, 6.1 ****

For the IRIX operating system versions 5.2, 5.3, 6.0, 6.0.1, and 6.1 an inst-able patch has been generated and made available via anonymous FTP and your service/support provider. The patch is number 1146 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) or its mirror, ftp.sgi.com. Patch 1146 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
~ftp/Patches/6.1

Checksums

The actual patch will be a tar file containing the following files:

Filename: patchSG0001146

Algorithm #1 (sum -r):15709 3 patchSG0001146

Algorithm #2 (sum): 16842 3 patchSG0001146

MD5 checksum: 055B660E1D5C1E38BC3128ADE7FC9A95

Filename: patchSG0001146.eoe1_man

Algorithm #1 (sum -r):26276 76 patchSG0001146.eoe1_man

Algorithm #2 (sum): 1567 76 patchSG0001146.eoe1_man

MD5 checksum: 883BC696F0A57B47F1CBAFA74BF53E81

Filename: patchSG0001146.eoe1_sw

Algorithm #1 (sum -r):61872 382 patchSG0001146.eoe1_sw

Algorithm #2 (sum): 42032 382 patchSG0001146.eoe1_sw

MD5 checksum: 412AB1A279A030192EA2A082CBA0D6E7

Filename: patchSG0001146.idb

Algorithm #1 (sum -r):39588 4 patchSG0001146.idb

Algorithm #2 (sum): 10621 4 patchSG0001146.idb

MD5 checksum: 259DD47E4574DAF9041675D64C39102E

Past SGI Advisories and security patches can be obtained via anonymous FTP from

ftp://sgigate.sgi.com

or its mirror

ftp://ftp.sgi.com

Sun Microsystems, Inc.

Included below is information concerning sendmail patches as outlined in Sun Microsystems Security Bulletin: #00133, 8 March 1996. The complete bulletin is available from ftp://ftp.cert.org/pub/vendors/sun/sun_bulletin_00133.

Here are our estimates for the availability of fixes incorporating into sendmail more strenuous checks against name-server-based attacks.

Note that the upcoming SunOS 4.1.x patches will represent the first backport of sendmail 8.6.x to those platforms, and will probably be assigned new patch numbers (instead of being recorded as revisions of the existing patches).

OS version	Est. date
5.6	in 5.6 FCS release
5.5.1	in 5.5.1 FCS release
5.5	Apr '96
5.4	Apr '96
5.3	Apr '96
4.1.4	May '96
4.1.3_U1	May '96
4.1.3	May '96

List of Current Sendmail Patches

Until the patches listed above are available, Sun recommends that every customer run the following sendmail patches on their systems.

A. Current sendmail patches

The latest sendmail patch for each supported version of SunOS is shown below. All current SunOS 5.x patches are based on sendmail V8; all SunOS 4.1.x patches are currently based on sendmail V5.

[Note that no sendmail patches exists for SunOS 5.5 and SunOS 5.5_x86. All earlier fixes were built into these releases.]

OS version	Patch ID	Released
5.4_x86	102064-05	19 Jan 96
5.4	102066-06	19 Jan 96

5.3	101739-08	19 Jan 96
4.1.4	102423-04	5 Oct 95
4.1.3_U1	101665-07	5 Oct 95
4.1.3	100377-22	5 Oct 95

Patch 100377-22 was issued jointly for SunOS 4.1.3 and SunOS 4.1.3c.

B. Obsolete sendmail patches

The following sendmail patches are now obsolete, and will no longer be maintained. Each is superseded by a patch listed above.

OS version	Patch ID	Released
5.4_x86	102320-01	26 May 95
5.4	102319-01	26 May 95
5.3	101235-01	1 May 95
5.3 (sic)	101371-04	9 Feb 94
4.1.4	102356-01	22 Feb 95
4.1.3_U1	101436-08	28 Oct 94
4.1.3	100224-13	28 Oct 94

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
102064-05.tar.Z	08423 335 16923	669	2816EF17F40E2FA5E8260CD98D349875
102066-06.tar.Z	62613 385 52067	770	666E6D6075E40D2BFDB539830EF1BCDA
101739-08.tar.Z	60842 385 28595	770	369D4E0758672ADCDAD2219179B8A062
102423-04.tar.Z	40900 216 33691	432	022B546A882B42FF826FE28429B2EDD8
101665-07.tar.Z	44656 216 37045	43	86F942F8CCBAD905AB2AE8CA33490D2B
100377-22.tar.Z	39051 214 58206	42	7B55564E6104FABAD7283DAE1CDD3D4A

The checksums shown above are from the BSD-based checksum (on 4.1.x, /bin/sum; on SunOS 5.x, /usr/ucb/sum) and from the SVR4 version on on SunOS 5.x (/usr/bin/sum).

The CERT Coordination Center thanks Eric Allman of Pangaea Reference Systems, Andrew Gross of San Diego Supercomputer Center, Eric Halil of AUSCERT, Wolfgang Ley of DFN-CERT, and Paul Vixie for their support in the development of this advisory.

Revision History

Apr. 28, 1998 Corrected URL for obtaining RFCs. Removed obsolete references to a latest_sw_versions directory.

Sep. 24, 1997 Updated copyright statement

June 4, 1997 Updated the URL pointing to the current version of BIND.

Aug. 30, 1996 Incorporated changes from CA-96.04.README into the advisory.

July 01, 1996 Introduction - added pointer to BIND 4.9.4.

Mar. 29, 1996 Introduction - updated information about the next release of BIND

Updates section - added isValid.c program information.

Appendix, Sun - added information from Sun.

Feb. 28, 1996 Appendix, SGI - added information.

5 CA-1996-05: Java Implementations Can Allow Connections to an Arbitrary Host

Original issue date: March 5, 1996
Last revised: September 24, 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 implementations of the Java Applet Security Manager. This vulnerability is present in the Netscape Navigator 2.0 Java implementation and in Release 1.0 of the Java Developer's Kit from Sun Microsystems, Inc. These implementations do not correctly implement the policy that an applet may connect only to the host from which the applet was loaded.

The CERT Coordination Center recommends installing patches from the vendors, and using the workaround described in Section III until patches can be installed.

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

Although our CA-96.05 CERT advisory does not discuss JavaScript, there have been a series of recent postings to newsgroups concerning a vulnerability in the way Netscape Navigator (Version 2.0) supports JavaScript.

As a clarification to our readers, this problem is different from the problem described in advisory CA-96.05.

Netscape Version 2.01 is now available. This version addresses the Java Applet Security Manager and the JavaScript problems recently discussed. For additional information about these issues and to obtain the new release, please see: http://home.netscape.com/eng/mozilla/2.01/relnotes/.

I. Description

There is a serious security problem with the Netscape Navigator 2.0 Java implementation. The vulnerability is also present in the Java Developer's Kit 1.0 from Sun Microsystems, Inc. The restriction allowing an applet to connect only to the host from which it was loaded is not properly enforced. This vulnerability, combined with the subversion of the DNS system, allows an applet to open a connection to an arbitrary host on the Internet.

In these Java implementations, the Applet Security Manager allows an applet to connect to any of the IP addresses associated with the name of the computer from which it came. This is a weaker policy than the stated policy and leads to the vulnerability described herein.

II. Impact

Java applets can connect to arbitrary hosts on the Internet, including those presumed to be previously inaccessible, such as hosts behind a firewall. Bugs in any TCP/IP-based network service can then be exploited. In addition, services previously thought to be secure by virtue of their location behind a firewall can be attacked.

III. Solution

To fix this problem, the Applet Security Manager must be more strict in deciding which hosts an applet is allowed to connect to. The Java system needs to take note of the actual IP address that the applet truly came from (getting that numerical address from the applet's packets as the applet is being loaded), and thereafter allow the applet to connect only to that same numerical address.

We urge you to obtain vendor patches as they become available. Until you can install the patches that implement the more strict applet connection restrictions, you should apply the workarounds described in each section below.

A. Netscape users

For Netscape Navigator 2.0, use the following URL to learn more about the problem and how to download and install a patch: http://home.netscape.com/newsref/std/java_security.html.

Until you install the patch, disable Java using the "Security Preferences" dialog box.

B. Sun users

A patch for Sun's HotJava will be available soon.

Until you can install the patch, disable applet downloading by selecting "Options" then "Security...". In the "Enter desired security mode" menu, select the "No access" option.

In addition, select the "Apply security mode to applet loading" to disable applet loading entirely, regardless of the source of the applet.

C. Both Netscape and Sun users

If you operate an HTTP proxy server, you could also disable applets by refusing to fetch Java ".class" files.

The CERT Coordination Center thanks Drew Dean, Ed Felton, and Dan Wallach of Princeton University for providing information for this advisory. We thank Netscape Communications Corporation, especially Jeff Truehaft, and Sun Microsystems, Inc., especially Marianne Mueller, for their response to this problem.

Revision History

Sep. 24, 1997 Updated copyright statement

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

Mar. 15, 1996 Introduction - added clarification on JavaScript and pointers to Netscape Version 2.01.

6 CA-1996-06: Vulnerability in NCSA/Apache CGI example code

Original issue date: March 20, 1996
Last revised: September 24, 1997
Updated copyright statement

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

The text of this advisory was originally released on March 14, 1996, as AUSCERT Advisory AA-96.01, developed by the Australian Computer Emergency Response Team. Because of the seriousness of the problem, we are reprinting the AUSCERT advisory here with their permission. Only the contact information at the end has changed: AUSCERT contact information has been replaced with CERT/CC contact information.

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

Note: The vulnerability described in this advisory is being actively exploited.

The Australian Computer Emergency Response Team (AUSCERT) has received information that example CGI code, as found in the NCSA 1.5a-export and APACHE 1.0.3 httpd (and possibly previous distributions of both servers), contains a security vulnerability. Programs using this code may be vulnerable to attack.

The CGI program "phf", included with those distributions, is an example of such a vulnerable program. This program may have been installed as part of the installation process for the httpd.

AUSCERT recommends that sites that have installed any CGI program incorporating the vulnerable code (such as "phf") apply one of the workarounds as described in Section 3.

1. Description

A security vulnerability has been reported in example CGI code, as provided with the NCSA httpd 1.5a-export and APACHE httpd 1.0.3 (and possibly previous distributions of both servers). The example code contains a library function escape_shell_cmd() (in cgi-src/util.c). This function, which attempts to prevent exploitation of shell-based library calls, such as system() and popen(), contains a vulnerability.

Any program which relies on escape_shell_cmd() to prevent exploitation of shell-based library calls may be vulnerable to attack.

In particular, this includes the "phf" program which is also distributed with the example code. Some sites may have installed phf by default, even though it is not required to run httpd successfully.

Any vulnerable program which is installed as a CGI application may allow unauthorised activity on the HTTP server.

Please note that this vulnerability is not in httpd itself, but in CGI programs which rely on the supplied escape_shell_cmd() function. Any HTTP server (not limited to NCSA or Apache) which has installed CGI programs which rely on escape_shell_cmd() may be vulnerable to attack.

Sites which have the source code to their CGI applications available can determine whether their applications may be vulnerable by examining the source for usage of the escape_shell_cmd() function which is defined in cgi-src/util.c.

Sites which do not have the source code for their CGI applications should contact the distributors of the applications for more information.

It is important to note that attacks similar to this may succeed against any CGI program which has not been written with due consideration for security. Sites using HTTP servers, and in particular CGI applications, are encouraged to develop an understanding of the security issues involved. References in Section 4 provide some initial pointers in this area.

2. Impact

A remote user may retrieve any world readable files, execute arbitrary commands and create files on the server with the privileges of the httpd process which answers HTTP requests. This may be used to compromise the http server and under certain configurations gain privileged access.

3. Workarounds

The use of certain C library calls (including system() and popen()) in security critical code (such as CGI programs) has been a notorious source of security vulnerabilities. Good security coding practice usually dictates that easily exploitable system or library calls should not be used. While secure CGI coding techniques are beyond the scope of this advisory many useful guidelines are available.

Sites planning to install or write their own CGI programs are encouraged to read the references in Section 4 first.

3.1. Remove CGI programs

Any CGI program which uses the escape_shell_cmd() function and is not required should be disabled. This may be accomplished by removing execute permissions from the program or removing the program itself.

In particular, sites which have installed the "phf" program and do not require it should disable it. The "phf" program is not required to run httpd successfully. Sites requiring "phf" functionality should apply one of the workarounds given in sections 3.2 and 3.3.

3.2. Rewrite CGI programs

The intent of the escape_shell_cmd() function is to prevent passing shell meta-characters to susceptible library calls. A more secure approach is to avoid the use of these library calls entirely.

AUSCERT recommends that sites which are currently using CGI programs which use shell-based library calls (such as system() and popen()) consider rewriting these programs to remove direct calls to easily compromised library functions.

Sites should note that this is only one aspect of secure programming practice. More details on this approach and other guidelines for secure CGI programming may be found in the references in Section 4.

3.3. Recompile CGI programs with patched util.c

For sites that still wish to use programs using the escape_shell_cmd() function, a patched version of cgi-src/util.c has been made available by NCSA which addresses this particular vulnerability. The patched version of util.c is available as part of the http1.5.1b3-export distribution. This is available from: http://hoohoo.ncsa.uiuc.edu/beta-1.5.

Please note that this is a beta-release of the NCSA httpd and is not a stable version of the httpd. The patched version of cgi-src/util.c may be used independently.

CGI programs which are required and use the escape_shell_cmd() should be recompiled with the new version of cgi-src/util.c and then reinstalled.

Apache have reported that they intend to fix this vulnerability in a future release. Until then the patched version of util.c as supplied in the http1.5.1b3-export release should be compatible.

4. Additional measures

Sites should consider taking this opportunity to examine their httpd configuration. In particular, all CGI programs that are not required should be removed, and all those remaining should be examined for possible security vulnerabilities.

It is also important to ensure that all child processes of httpd are running as a non-privileged user. This is often a configurable option. See the documentation for your httpd distribution for more details.

Numerous resources relating to WWW security are available. The following pages provide a useful starting point. They include links describing general WWW security, secure httpd setup and secure CGI programming.

The World Wide Web Security FAQ:
http://www-genome.wi.mit.edu/WWW/faqs/www-security-faq.html.

NSCA's "Security Concerns on the Web" Page: http://hoohoo.ncsa.uiuc.edu/security/.

The following book contains useful information including sections on secure programming techniques.

Practical Unix & Internet Security, Simson Garfinkel and Gene Spafford, 2nd edition, O'Reilly and Associates, 1996.

Please note that the URLs referenced in this advisory are not under AUSCERT's control and therefore AUSCERT cannot be responsible for their availability or content. Please contact the administrator of the site in question if you encounter any difficulties with the above sites.

AUSCERT thanks Jeff Uphoff of NRAO, IBM-ERS, NASIRC and Wolfgang Ley of DFN-CERT for their assistance.

UPDATES

Similar attacks may succeed against other cgi scripts if the scripts are written without appropriate care regarding security issues. We encourage sites to evaluate all programs in their cgi-bin directory and remove any scripts that are not in active use.

We would like to point out that along with "phf" we have received reports that "php" programs are also being exploited.

CERT/CC received the following update from NASIRC concerning the vulnerability described in this advisory:

NEW INFORMATION

The routine "escape_shell_cmd()" also occurs in the file "src/util.c". Note that the files "cgi-src/util.c" and "src/util.c" are not identical, however they both contain an identical copy of the routine "escape_shell_cmd()", which has the vulnerability. The file "src/util.c" is used to build the HTTP daemon, therefore the "newline" hole exists within the server.

PATCH

The patch recommended by NCSA modifies the routine

"escape_shell_cmd()" to expand the list of characters that it will escape. In the routine "escape_shell_cmd()", the line:

```
if(ind("&;`'\"|*?~<>^()[]{}$\\",cmd[x]) != -1){
```

Must be changed to:

```
if(ind("&;`'\"|*?~<>^()[]{}$\\\n",cmd[x]) != -1){
```

NCSA HTTPD 1.5.1

Instead of patching the source, the most up-to-date version of NCSA HTTPd source may be downloaded from:
ftp://ftp.ncsa.uiuc.edu/Web/httpd/Unix/ncsa_httpd/current/httpd_1.5.1-export_source.tar.Z.

MD5 (httpd_1.5.1-export_source.tar.Z) = bcf1fd410b5839c51dc75816a155fbb8

Revision History

Sep. 24, 1997 Updated copyright statement

June 4, 1997 Updates section - added information about other cgi programs being exploited.

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

Apr. 17, 1996 Updates section - added new information provided by the NASA Automated Systems Incident Response Capability (NASIRC).

7 CA-1996-07: Weaknesses in Java Bytecode Verifier

Original issue date: March 29, 1996
Last revised: September 24, 1997
Updated copyright statement

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

The CERT Coordination Center has received reports of weaknesses in the bytecode verifier portion of Sun Microsystems' Java Development Kit (JDK) versions 1.0 and 1.0.1. The JDK is built into Netscape Navigator 2.0 and 2.01. We have not received reports of the exploitation of this vulnerability.

When applets written with malicious intent are viewed, those applets can perform any operation that the legitimate user can perform on the machine running the browser. For example, a maliciously written applet could remove files from the machine on which the browser is running--but only if the legitimate user could also.

Problem applets have to be specifically written with malicious intent, and users are at risk only when connecting to "untrusted" web pages. If you use Java-enabled products on a closed network or browse the World Wide Web but never connect to "untrusted" web pages, you are not affected.

The CERT staff recommends disabling Java in Netscape Navigator and not using Sun's appletviewer to browse applets from untrusted sources until patches are available from these vendors. We further recommend upgrading to Netscape 2.02 but still disabling Java and JavaScript if you don't need these programs.

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 Java Programming Language is designed to allow an executable computer program, called an applet, to be attached to a page viewable by a World Wide Web browser. When a user browsing the Web visits that page, the applet is automatically downloaded onto the user's machine and executed, but only if Java is enabled.

It is possible for an applet to generate and execute raw machine code on the machine where the browser is running. This means that a maliciously written applet can perform any action that the legitimate user can perform; for example, an applet can read, delete, or change files that the user owns. Because applets are loaded and run automatically as a side-effect of visiting a Web page, someone could "booby-trap" their Web page and compromise the machine of anyone visiting the page. This is the problem described in the Wall Street Journal on March 26, 1996 ("Researchers Find Big Security Flaw in Java Language," by Don Clark).

Note: The security enhancements announced by Sun Microsystems in JDK version 1.0.1 and by Netscape Communications in Netscape Navigator version 2.01 do *not* fix this flaw.

II. Impact

If Java is enabled and a Web page containing a maliciously written applet is viewed by any of the vulnerable browsers or Sun's appletviewer, that applet can perform any operation that the legitimate user can perform. For example, the applet could read, delete, or in other ways corrupt the user's files and any other files the user has access to, such as /etc/passwd.

III. Solution

We recommend obtaining vendor patches as soon as they become available. Until you can install the patches, we urge you to apply the workarounds described below.

A. Java Development Kit users

Sun reports that source-level fixes will be supplied to source licensees in the next few days. The fixes will also be included in the next JDK version, v1.0.2, which will be released within the next several weeks.

The JDK itself is a development kit, and it can safely be used to develop applets and applications. If you choose to use the appletviewer as a rudimentary browser, do not use it to browse applets from untrusted sources until you have installed the v1.0.2 browser.

B. Netscape users

Upgrade to Netscape version 2.02, which addresses the Java Bytecode Verifier problems discussed in the advisory.

Until you can do so, if you use Netscape 2.0 or 2.01, disable Java using the "Security Preferences" dialog box. You do not need to disable JavaScript as part of this workaround.

After you update to version 2.02, you should still disable Java and JavaScript if these programs are not being used. (This also applies to Netscape Version 3.0b4.) Note that in order to display Netscape's home page, you must have JavaScript enabled.

For the latest news about fixes for Netscape Navigator, consult the following for details: http://home.netscape.com/.

Netscape 2.02 and additional information about it are available from http://home.netscape.com/eng/mozilla/2.02/relnotes/.

IV. Information for HotJava (alpha3) users

Sun Microsystems has provided the following information for users of HotJava (alpha3).

Sun made available last year a demonstration version of a browser called "HotJava." That version (alpha3) is proof-of-concept software only, not a product. HotJava (alpha3) uses an entirely different security architecture from JDK 1.0 or JDK 1.0.1. It will not be tested for any reported security vulnerabilities that it might be susceptible to, and Sun neither supports it nor recommends its use as a primary browser. When HotJava is released as a product, it will be based on an up-to-date version of the JDK and fully supported.

V. Information for Macintosh users

Macintosh version 2.01 does not support Java, so there is nothing to disable as part of the solution to the problems described in this advisory.

The CERT Coordination Center thanks Drew Dean, Ed Felten, and Dan Wallach of Princeton University for providing information for this advisory. We thank Netscape Communications Corporation and Sun Microsystems, Inc. for their response to this problem.

Revision History

```
Sep. 24, 1997 Updated copyright statement

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

June 26, 1996 Introduction - added a note about Netscape 2.02.
              Sec.III.B - added a pointer to Netscape 2.02 and a
              recommendation about disabling Java and JavaScript.

Apr. 1, 1996 Sec. III.B - added a note about viewing
             Netscape's home page.
             Sec. V - added this section for Macintosh users.
```

8 CA-1996-08: Vulnerabilities in PCNFSD

Original issue date: April 18, 1996
Last revised: December 5, 1997
Updated information for NCR Corporation.

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

The CERT Coordination Center has received reports of two vulnerabilities in the pcnfsd program (pcnfsd is also known as rpc.pcnfsd); we have also received reports that these problems are being exploited. These vulnerabilities are present in some vendor-provided versions of pcnfsd and in some publicly available versions.

These two vulnerabilities were reported by Avalon Security Research in reports entitled "pcnfsd."

If you are using a vendor-supplied version of pcnfsd, please see the vendor information in Section III.A and Appendix A. Until you can install a patch from your vendor for these vulnerabilities, consider using the publicly available version described in Section III.B.

If you already use or plan to switch to a public version, we urge you to use the version cited in Section III.B or install the patch described in Section III.C. This patch has already been incorporated into the pcnfsd version described in III.B. There are many different public domain versions of pcnfsd, and we have not analyzed the vulnerability of those versions. We have analyzed and fixed the problems noted in this advisory only in the version described in III.B.

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 pcnfsd program (also called rpc.pcnfsd) is an authentication and printing program that runs on a UNIX server. There are many publicly available versions, and several vendors supply their own version.

pcnfsd supports a printing model that uses NFS to transfer files from a client to the pcnfsd server. (Note: pcnfsd does *not* provide NFS services.) When a client wants to print a file, it requests the path to a spool directory from the server. The client then writes the necessary files for printing using NFS, and informs the pcnfsd server that the files are ready for printing.

pcnfsd creates a subdirectory for each of its clients using the client's hostname, then returns this path name to the client. The returned path name must be exported via to its clients by the NFS server. The NFS server and the pcnfsd server may be two separate machines.

The first vulnerability is that pcnfsd, which runs as root, creates the aforementioned directories with *mkdir(2)* and then changes their mode with *chmod(2)* to mode 777. If the target directory is

replaced with a symbolic link pointing to a restricted file or directory, the *mkdir(2)* will fail but the *chmod(2)* will succeed. This means that the target of the symbolic link will be mode 777.

Note that pcnfsd must run as root when servicing print requests so that it can assume the identity of the PC user when interacting with UNIX print commands. On some systems, pcnfsd may also have to run as root so it can read restricted files when carrying out authentication tasks.

The second vulnerability is that pcnfsd calls the *system(3)* subroutine as root, and the string passed to *system(3)* can be influenced by the arguments given in the remote procedure call. Remote users can execute arbitrary commands on the machine where pcnfsd runs.

II. Impact

For the first vulnerability, local users can change the permissions on any file accessible to the local system that the root user can change. For the second vulnerability, remote users can execute arbitrary commands as root on the machine where pcnfsd runs.

The impact is that directories can become world writable (mode 777). What this can lead to is bounded by the creativity of the intruder. For example, once the mode of /etc were changed to mode 777, one could then replace the password file, and then go on from there.

Exploitation of these vulnerabilities is only part of a larger attack scenario. Once exploited, there are many pathologies that could follow.

III. Solution

If you are using pcnfsd from a vendor, consult the vendor list in Section A. If your vendor is not listed, we recommend that you contact your vendor directly.

Until a vendor patch is available, we recommend that you obtain the publicly available version of pcnfsd as described in Section B. This version already has the patch described in Section C.

If you are presently using a public version of pcnfsd, we recommend that you either change to the version listed in Section B or apply the patch described in Section C. (The version in Section B already contains this patch.)

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

Below is a list of the vendors who have reported to us as of the date of this advisory. More complete information, is provided in the appendix. We will update the appendix as we receive more information.

If your vendor's name is not on this list, please contact the vendor directly.

Vendor or Source	Status
BSDI BSD/OS	Vulnerable. Patch available.

Vendor or Source	Status
Hewlett Packard	Vulnerable. Patch under development.
IBM AIX 3.2	Vulnerable. Patches available.
IBM AIX 4.1	Vulnerable. Patches available.
NCR Corporation	Vulnerable. Patches available.
NEXTSTEP	Vulnerable. Will be fixed in version 4.0.
SCO OpenServer 5	Vulnerable. Patch under development.
SC UnixWare 2.1	Vulnerable. Patch under development.
SCO UnixWare 2.1	Vulnerable. Patch under development.
SGI IRIX 5.3	Vulnerable. Patch under development.
SGI IRIX 6.2	Not vulnerable.

B. Until you are able to install the appropriate patch, we recommend that you obtain a version of pcnfsd from one of the following locations.

This version already has the patch mentioned in Section III.C.

ftp://ftp.cert.org/pub/tools/pcnfsd/pcnfsd.93.02.16-cert-dist.tar.Z
ftp://ftp.cert.dfn.de/pub/tools/net/pcnfsd/pcnfsd.93.02.16-cert-dist.tar.Z

MD5 (pcnfsd.93.02.16-cert-dist.tar.Z) = b7af99a07dfcf24b3da3446d073f8649

Build, install, and restart rpc.pcnfsd.

Ensure that the mode of the top-level pcnfsd spool directory is 755. In this version of pcnfsd, the top level spool directory is /usr/spool/pcnfs. To change this to mode 755, do the following as root:

```
chmod 755 /usr/spool/pcnfs
```

C. A patch is available for the two vulnerabilities described in this advisory.

Apply the patch using the GNU patch utility or by hand as necessary. Rebuild, reinstall, and re-start rpc.pcnfsd. Set the mode of the top-level pcnfsd spool directory to 755.

For example, in the version of pcnfsd cited in Section B, the top level spool directory is /usr/spool/pcnfs. To change this to mode 755, do the following as root:

```
chmod 755 /usr/spool/pcnfs
```

Below is the location of a version of the patch that is an improvement over the patch originally cited in the advisory. The modifications are in the suspicious() function in pcnfsd_misc.c., courtesy of Sun Microsystems, Inc.

To prevent any confusion concerning the checksums, please see the file README.pcnfsd.93.02.16-cert. Checksums are also included below:

ftp://ftp.cert.org/pub/tools/pcnfsd/README.pcnfsd.93.02.16-cert
MD5 (README.pcnfsd.93.02.16-cert) = 07c64cd714bfaab3eb3849439a615b79

ftp://ftp.cert.org/pub/tools/pcnfsd/pcnfsd.93.02.16-cert-dist.tar.Z
MD5 (pcnfsd.93.02.16-cert-dist.tar.Z) = dc9b50172dfba8e6f9ad0c83f0e087e8

Note: When the above file is unpacked, the md5 checksum referenced in the README.pcnfsd.93.02.16-cert matches the following:

MD5 (pcnfsd.93.02.16-cert.tar) = 3a33f392d66b166cbc630275d8aba6f7

ftp://ftp.cert.org/pub/tools/pcnfsd/pcnfsd_misc.c-diffs
MD5 (pcnfsd_misc.c-diffs) = e9a83e6d540ab4683767ecf6d66dda9d

ftp://ftp.cert.org/pub/tools/pcnfsd/pcnfsd_print.c-diffs
MD5 (pcnfsd_print.c-diffs) = 7d9dac3c14b258e855517894e2934b14

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.

Berkeley Software Design, Inc. (BSDI)

The problem described in these vulnerabilities is present in all versions of BSD/OS. There is a patch (our patch number U210-007) for our 2.1 version of BSD/OS and associated products available from our patch and ftp servers <patches@BSDI.>
or ftp://ftp.BSDI.COM/bsdi/patches/patches-2.1/U210-007.

Data Design Systems, Inc.

The Tandem NonStop Kernel (NSK) system, does NOT contain either of the vulnerabilities cited in the advisory.

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.

FreeBSD Inc.

There are two separate ways of upgrading. The patch listed below is a source code patch, and is available from:
ftp://ftp.FreeBSD.ORG/pub/FreeBSD/FreeBSD-current/ports/net/pcnfsd/patches/patch-ad
MD5 (patch-ad) = 6dfdf6229632e53cb060961ac09bbd1a

This is part of the ports collection and anyone using current revisions of the ports system will automatically have this patch applied.

You can also get a FreeBSD "package" (pre-compiled binary) from:

ftp://ftp.FreeBSD.ORG/pub/FreeBSD/packages-current/net/pcnfsd-93.02.16.tgz
MD5 (pcnfsd-93.02.16.tgz) = 59c54dae46d1b4fd41887877b0a7097a

Hewlett-Packard Company

1. The rpc.pcnfsd binary that ships with HP systems contains a vulnerability that could allow a user to change permissions on a restricted file or directory.

Hewlett Packard is delivering a set of operating system dependent patches which contain a new version of rpc.pcnfsd. Accompanying each patch is a README file which discusses the general purpose of the patch and describes how to apply it to your system.

Recommended solution:

Apply one of the following patches based on your system hardware and operating system revision:

s300/s400 9.X - PHNE_7371 (rpc.pcnfsd)
s700/s800 9.X - PHNE_7072 (NFS Megapatch)
s700/s800 10.X - PHNE_7073 (NFS Megapatch)

The patches described above provide a new version of the rpc.pcnfsd executable which fixes the vulnerability.

2. The rpc.pcnfsd binary that ships with most Unix systems contains a vulnerability that could allow users to execute arbitrary commands on the machine where pcnfsd runs.

The rpc.pcnfsd daemon that ships with Hewlett Packard systems does not make the system call that allows this vulnerability. Since HP systems are not vulnerable - there is no fix!

To subscribe to automatically receive future NEW HP Security Bulletins please refer to information in ftp://ftp.cert.org/pub/vendors/hp/HP.contact_info.

IBM Corporation

See the appropriate release below to determine your action.

Until these fixes are applied, pcnfsd should be turned off and commented out in /etc/inetd.conf.

WARNING: If the line in /etc/inetd.conf has only one comment character, it will be uncommented (and exploitable) when mknfs is run! The inetd.conf entry must look like the following to remain turned off:

pcnfsd sunrpc_udp udp wait root /usr/sbin/rpc.pcnfsd pcnfsd 150001 1-2

AIX 3.2

Apply the following fix to your system:
APAR - IX68084 (PTF - U447684 U450406)

To determine if you have this PTF on your system, run the following command:
lslpp -lB U447684 U450406

AIX 4.1

Apply the following fix to your system:
APAR - IX68086

To determine if you have this APAR on your system, run the following command:
instfix -ik IX68086

Or run the following command:
lslpp -h bos.net.nfs.client bos.net.nis.server

Your version of bos.net.nfs.client should be 4.1.5.5 or later. Your version of bos.net.nis.server should be 4.1.5.1 or later.

AIX 4.2

Apply the following fix to your system:
APAR - IX68087

To determine if you have this APAR on your system, run the following command:
instfix -ik IX68087

Or run the following command: lslpp -h bos.net.nfs.client bos.net.nis.server

Your version of bos.net.nfs.client should be 4.2.1.1 or later. Your version of bos.net.nis.server should be 4.2.1.3 or later.

To Order

APARs may be ordered using Electronic Fix Distribution (via FixDist) or from the IBM Support Center. For more information on FixDist, reference http://service.software.ibm.com/aixsupport/ or send e-mail to aixserv@austin.ibm.com with a subject of "FixDist".

IBM and AIX are registered trademarks of International Business Machines Corporation.

NCR Corporation

The pcnfsd binary that shipped with some older NCR MP-RAS SVR4 releases contains a vulnerability that could allow a user to change permissions on a restricted file or directory.

NCR is delivering a set of operating system dependent patches which contain a new version of pcnfsd. Accompanying each patch is a README file which discusses the general purpose of the patch and describes how to apply it to your system.

Recommended solution:

Apply one of the following patches based on your operating system revision:

MP-RAS 2.03.x - PNFS203 (Version after 5/24-96)
MP-RAS 3.00.x - PNFS300 (Version after 5/28-96)
MP-RAS 3.01.x and later - Not vulnerable

The patches described above provide a new version of the pcnfsd executable which fixes the vulnerability.

NEC Corporation

Some systems are vulnerable and patches are available through anonymous FTP from ftp://ftp.meshnet.or.jp in the /pub/48pub/security directory.

UP-UX/V (Rel4.2MP)	R5.x	NECu5s003.COM.pkg /pub/48pub/security/up/r5/pkg Results of sum = 3060 266 md5 = 79E626B99A55FB0DBCE6EE642874570A
	R6.x	NECu6s003.COM.pkg /pub/48pub/security/up/r6/pkg Results of sum = 47304 272 md5 = 9FC9E993A5AB51291BF4817D3D70FBFD
	R7.x	NECu7s003.COM.pkg /pub/48pub/security/up/r7/pkg Results of sum = 46470 291 md5 = 59CA6887078AF88EA165AFD3BF5A1374
EWS-UX/V (Rel4.2)	R7.X	NECe7s004.COM.pkg /pub/48pub/security/ews/r7/pkg Results of sum = 3827 194 md5 = 4D40D9258DAB7EA41C30789609818330
	R8.x	NECe8s004.COM.pkg /pub/48pub/security/ews/r8/pkg Results of sum = 24399 199 md5 = 40B4CB1140791C14D1B604B6E8CB5FCB

	R9.x (except EWS4800/110N)	NECe9s008.COM.pkg /pub/48pub/security/ews/r9/pkg Results of sum = 23250 203 md5 = 5AD8BED137AAE7D0067EF3120574786C
	R9.x (EWS4800/110N)	NECe9s007.COM.pkg /pub/48pub/security/ews/r9n/pkg Results of sum = 3972 201 md5 = 28B2FA99F5200F81C5465571EF27E08B
	R10.x	NECeas004.COM.pkg /pub/48pub/security/ews/ran/pkg Results of sum = 51969 205 md5 = B6E12017E66DC8DC38FBE78CA1F0B0F0
EWS-UX/V (Rel4.2MP)	R10.x	NECmas007.COM.pkg /pub/48pub/security/ews/ra/pkg Results of sum = 48060 291 md5 = 42F8AE832071F033E21D8718A3670D76
UX/480O	R11.x	NECmbs010.COM.pkg /pub/48pub/security/ews/rb/pkg Results of sum = 24885 335 md5 = 7A14CBE4EA9B2470E340B5EEFD523F95

For further information contact: UX48-security-support@nec.co.jp . We encourage you contact the vendor directly if you have any questions.

NeXT Software, Inc.

NEXTSTEP is vulnerable. This will be fixed in the 4.0 release of OpenStep for Mach (aka NEXTSTEP 4.0, due out 2Q96).

Novell

CERT staff do not know whether Novell's enhanced version of PCNFSD (LWPNFSD) is vulnerable to this problem. We encourage you contact the vendor directly if you have any questions.

The Santa Cruz Operation, Inc.

Patches for pcnfsd are currently being developed for the following releases:

SCO OpenServer 5
SCO UnixWare 2.1.

These releases, as well as all prior releases, are vulnerable to both issues mentioned in the advisory. Should you not need to use pcnfs, SCO recommends that you not run pcnfsd. This can be done by commenting out pcnfsd in the appropriate script that starts pcnfsd, located in /etc/rc2.d.

This CERT advisory will be updated when further patch information is available.

Silicon Graphics Corporation

pcnfsd was only released for IRIX 5.3 and IRIX 6.2.

SGI is producing patch1179 for IRIX 5.3.

IRIX 6.2 is not vulnerable.

Sun Microsystems, Inc.

Sun has made patches available:

Solaris 2.4, 2.5 (Sparc) 103095-02
Solaris 2.4, 2.5 (X86) 103457-01
SunOS 4.1.X 103096-02

TGV Software, Inc./Cisco Systems, Inc.

These vulnerabilities are UNIX-specific and are not present in any version of MultiNet for OpenVMS.

The CERT Coordination Center thanks Josh Daymont, Ben G., and Alfred H. of Avalon Security Research for providing information for this advisory. We thank Wolfgang Ley of DFN-CERT for his help in understanding these problems.

Revision History

```
Dec. 5, 1997  Appendix A - Added information for NCR Corporation.

Oct. 31, 1997 Updated vendor information for IBM.

Sep. 24, 1997 Updated copyright statement

Apr. 03, 1997 Minor changes: corrected a name in the acknowledg-
ments; indicated that CERT is now a registered service mark

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

Appendix B was moved to Sec. III.C. Appendix A - updated IBM URL in
"To Order" section.

Aug. 01, 1996 Appendix A - updated Hewlett-Packard patch infor-
mation.

July 26, 1996 Appendix A - modified NEC patch information.
```

July 5, 1996 Appendix A - added pointer to updated vendor information for Digital Equipment Corporation.

June 26, 1996 Appendix A - updated vendor information for NEC.

Appendix A - added vendor information for Data Design Systems, Inc.

May 8, 1996 Appendix A - added patch information for FreeBSD.

May 6, 1996 Section II -added additional clarification about the impact of the vulnerability described.

Appendix B - replaced the patch information originally contained in Appendix B with updated information.

Appendix A - added updates for Digital Equipment Corporation, Novell, Sun Microsystems, Inc, and TGV Software, Inc./Cisco Systems, Inc.

Apr. 23, 1996 Appendix A - added information from NEC Corporation.

Apr. 19, 1996 Appendix B - new information on the fix referred to in Appendix B of the advisory.

9 CA-1996-09: Vulnerability in rpc.statd

Original issue date: April 24, 1996
Last revised: December 5, 1997
Added information for NCR Corporation.

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

The CERT Coordination Center has received reports of a vulnerability in rpc.statd (rpc.statd is also known as statd on some systems). We have received reports of this vulnerability being exploited.

If exploited, this vulnerability can be used to remove any file that the root user can remove or to create any file that the root user can create.

Section III and Appendix A contain information from vendors. Appendix B contains an example of a possible workaround.

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

I. Description

rpc.statd, also called statd, is the NFS file-locking status monitor. It interacts with rpc.lockd, also called lockd, to provide the crash and recovery functions for file locking across NFS.

Note that rpc.lockd and rpc.statd work together; if either is running, both must run.

rpc.lockd and rpc.statd can be safely turned off on a machine if that machine is neither an NFS client nor an NFS server. Consult your system documentation to learn how to turn these services off and not restart them when a system is rebooted.

If a machine where rpc.lockd and rpc.statd have been disabled becomes either an NFS server or an NFS client, then both rpc.lockd and rpc.statd should be turned back on.

NFS is stateless, which means that NFS clients and servers can be rebooted without a loss of file integrity due to NFS. In contrast, NFS file locking is stateful. To achieve this stateful nature in a stateless environment, rpc.lockd must work with rpc.statd to add state to file locking.

To understand what rpc.statd does, it is first necessary to understand what rpc.lockd does. rpc.lockd processes lock requests that are sent either locally by the kernel or remotely by another lock daemon. rpc.lockd forwards lock requests for remote NFS files to the NFS server's lock daemon using Remote Procedure Calls (RPC).

rpc.lockd then requests monitoring service from the status monitor daemon, rpc.statd, running on the NFS server. Monitoring services are needed because file locks are maintained in the NFS

server kernel. In the event of a system crash or reboot, all NFS locks would normally be lost. It is rpc.statd that adds stateful file locking.

When an NFS server reboots, rpc.statd causes the previously held locks to be recovered by notifying the NFS client lock daemons to resubmit previously granted lock requests. If a lock daemon fails to secure a previously granted lock on the NFS server, it sends SIGLOST to the process that originally requested the file lock.

The vulnerability in rpc.statd is its lack of validation of the information it receives from what is presumed to be the remote rpc.lockd. Because rpc.statd normally runs as root and because it does not validate this information, rpc.statd can be made to remove or create any file that the root user can remove or create on the NFS server.

II. Impact

Any file that root could remove can be removed by rpc.statd. Any file that root could create can be created by rpc.statd, albeit with mode 200.

III. Solution

The general solution to this problem is to replace the rpc.statd daemon with one that validates the information sent to it by the remote rpc.lockd. We recommend that you install a patch from your vendor if possible. If a patch is not available for your system, we recommend contacting your vendor and requesting that a patch be developed as soon as possible. In the meantime, consider whether the information in Appendix B is applicable to your site.

Vendor Information

Below is a list of vendors who have provided information. Details are in Appendix A of this advisory. We will update the advisory as we receive more information.

Berkeley Software Design, Inc.
Cray Research, Inc.
Data General Corporation
Harris Computer Systems Corp.
Hewlett-Packard Company
IBM Corporation
NCR Corporation
NEC Corporation
NeXT Software, Inc.
The Santa Cruz Operation
Silicon Graphics. Inc.
Sony Corporation
Sun Microsystems, Inc.
TGV/Cisco Systems, Inc.

If your vendor's name is not on this list, please contact the vendor directly.

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.

Apple Computer, Inc.

A/UX

An upgrade to A/UX version 3.1 (and 3.1.1) for this vulnerability is available. The upgrade replaces the rpc.statd binary with a new, improved version. It is available via anonymous FTP from ftp.support.apple.com:
pub/apple_sw_updates/US/Unix/A_UX/supported/3.x/rpc.statd/rpc.statd.Z.

Uncompress(1) this file and replace the existing version in /etc. Modify the entry for rpc.statd in /etc/inittab to "respawn" instead of "wait".

Kill the running rpc.statd and restart.

Earlier versions of A/UX are not supported by this patch. Users of previous versions are encouraged to update their system or disable rpc.statd.

AIX for the Apple Network Server

An upgrade to AIX version 4.1.4 for the Network Server which resolves this vulnerability is available. The PTF replaces the rpc.statd binary and related programs with new, improved versions.

To determine if you already have APAR IX55931 on your system, run the following command:

instfix -ik IX55931

Or run the following command:

lslpp -h bos.net.nfs.client

Your version of bos.net.nfs.client should be 4.1.4.7 or later.

The PTF for this APAR is available via anonymous FTP from ftp.support.apple.com:

pub/apple_sw_updates/US/Unix/AIX/supported/4.1/bos.net.nfs.client.bff

Place this file in /usr/sys/inst.images or another directory of your choice. To install the PTF, start smit using the following fast path:

smit install_selectable

Select the menu item "Install Fileset Updates by Fix" and provide the name of the directory in which the PTF was placed. Enter OK and in the next dialog, enter the APAR number, IX55931, in the "FIXES" item. For information about the other options in this dialog, see the manual page for *installp(1)*. Enter OK, exit smit and restart the system.

Customers should contact their reseller for any additional information.

Berkeley Software Design, Inc.

BSD/OS is not vulnerable.

Cray Research, Inc.

This problem has been tracked with SPR 99983 and reported with Field notice 2107. Since statd is only available on 9.0 systems fixes have been provided for UNICOS 9.0 and higher.

Data General Corporation

Data General has fixed this vulnerability in DG/UX R4.11 Maintenance Update 2 (R4.11MU02).

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.

Harris Computer Systems Corporation

All versions of NightHawk CX/SX and CyberGuard CX/SX are not vulnerable.

All versions of NightHawk CX/UX and PowerUX are vulnerable.
Users are advised, until patches are available, to use the workaround in the advisory.

Hewlett-Packard Company

The rpc.statd daemon that ships with HP systems contains a vulnerability that could allow a remote user to delete files on the system running rpc.statd.

Hewlett Packard is delivering a set of operating system dependent patches which contain a new version of rpc.statd. Accompanying each patch is a README file which discusses the general purpose of the patch and describes how to apply it to your system.

Recommended solution:

Apply one of the following patches based on your system hardware and operating system revision:

s300/s400 9.X - PHNE_7372 (rpc.statd)
s700/s800 9.X - PHNE_7072 (NFS Megapatch)
s700/s800 10.X - PHNE_7073 (NFS Megapatch)

The patches described above provide a new version of the rpc.statd executable which fixes the vulnerability.

To subscribe to automatically receive future NEW HP Security Bulletins please refer to information in ftp://ftp.cert.org/pub/vendors/hp/HP.contact_info.

IBM Corporation

See the appropriate release below to determine your action.

AIX 3.2

Apply the following fix to your system:

APAR - IX56056 (PTF - U441411)

To determine if you have this PTF on your system, run the following command:

lslpp -lB U441411

AIX 4.1

Apply the following fix to your system:

APAR - IX55931

To determine if you have this APAR on your system, run the following command:

instfix -ik IX55931

Or run the following command:

lslpp -h bos.net.nfs.client

To Order

APARs may be ordered using FixDist or from the IBM Support Center. For more information on FixDist, reference URL: http://service.software.ibm.com/aixsupport/ or send e-mail to aixserv@austin.ibm.com with a subject of "FixDist".

NCR Corporation

The statd binary that shipped with some older NCR MP-RAS SVR4 releases contains a vulnerability that could allow a remote user to create or delete files on a server running statd.

NCR is delivering a set of operating system dependent patches which contain a new version of statd. Accompanying each patch is a README file which discusses the general purpose of the patch and describes how to apply it to your system.

Recommended solution:

Apply one of the following patches based on your operating system revision:

MP-RAS 2.03.x - PNFS203 (Version after 7/26-96)
MP-RAS 3.00.x - PNFS300 (Version after 8/19-96)
MP-RAS 3.01.x and later - Not vulnerable

The patches described above provide a new version of the statd executable, which fixes the vulnerability.

NEC Corporation

Some systems are vulnerable and patches are available through anonymous FTP from ftp://ftp.meshnet.or.jp.

UP-UX/V (Rel4.2MP)	R5.x	NECu5s003.COM.pkg /pub/48pub/security/up/r5/pkg Results of sum = 3060 266 md5 = 79E626B99A55FB0DBCE6EE642874570A
	R6.x	NECu6s003.COM.pkg /pub/48pub/security/up/r6/pkg Results of sum = 47304 272 md5 = 9FC9E993A5AB51291BF4817D3D70FBFD
	R7.x	NECu7s003.COM.pkg /pub/48pub/security/up/r7/pkg Results of sum = 46470 291 md5 = 59CA6887078AF88EA165AFD3BF5A1374

EWS-UX/V (Rel4.2)	R7.X	NECe7s004.COM.pkg /pub/48pub/security/ews/r7/pkg Results of sum = 3827 194 md5 = 4D40D9258DAB7EA41C30789609818330
	R8.x	NECe8s004.COM.pkg /pub/48pub/security/ews/r8/pkg Results of sum = 24399 199 md5 = 40B4CB1140791C14D1B604B6E8CB5FCB
	R9.x (except EWS4800/110N)	NECe9s008.COM.pkg /pub/48pub/security/ews/r9/pkg Results of sum = 23250 203 md5 = 5AD8BED137AAE7D0067EF3120574786C
	R9.x (EWS4800/110N)	NECe9s007.COM.pkg /pub/48pub/security/ews/r9n/pkg Results of sum = 3972 201 md5 = 28B2FA99F5200F81C5465571EF27E08B
	R10.x	NECeas004.COM.pkg /pub/48pub/security/ews/ran/pkg Results of sum = 51969 205 md5 = B6E12017E66DC8DC38FBE78CA1F0B0F0
EWS-UX/V (Rel4.2MP)	R10.x	NECmas007.COM.pkg /pub/48pub/security/ews/ra/pkg Results of sum = 48060 291 md5 = 42F8AE832071F033E21D8718A3670D76
UX/480	R11.x	NECmbs010.COM.pkg /pub/48pub/security/ews/rb/pkg Results of sum = 24885 335 md5 = 7A14CBE4EA9B2470E340B5EEFD523F95

For further information contact: UX48-security-support@nec.co.jp. We encourage you contact the vendor directly if you have any questions.

NeXT Software, Inc.

This vulnerability will be fixed in release 4.0 of OpenStep for Mach, scheduled for 2Q96.

The Santa Cruz Operation, Inc.

These are not vulnerable:

SCO UnixWare 2.x.
SCO OpenServer 3.0, 5
SCO Open Desktop 2.x, 3.x
SCO NFS 1.x.x.

Silicon Graphics, Inc.

All versions of IRIX earlier than 6.2 are vulnerable.

IRIX 6.2 is not vulnerable.

The the most current information appears in ftp://sgigate.sgi.com/security/19960301-01-P.

Sony Corporation

```
NEWS-OS 4.2.1   vulnerable; Patch 0124 [rpc.statd] is available.

NEWS-OS 6.0.3   vulnerable; Patch SONYP6063 [lockd/statd 2] is
available.

NEWS-OS 6.1     vulnerable; Patch SONYP6176 [lockd/statd] is availa-
ble.

NEWS-OS 6.1.1   vulnerable; Patch SONYP6207 [lockd/statd] is availa-
ble.

Patches are available via anonymous FTP in the

/pub/patch/news-os/un-official directory on

ftp1.sony.co.jp [202.238.80.18]:

4.2.1a+/0124.doc        describes about patch 0124 [rpc.statd]

4.2.1a+/0124_C.pch      patch for NEWS-OS 4.2.1C/a+C

4.2.1a+/0124_R.pch      patch for NEWS-OS 4.2.1R/RN/RD/aRD/aRS/a+R

6.0.3/SONYP6063.doc     describes about patch SONYP6063 [lockd/statd
2]

6.0.3/SONYP6063.pch     patch for NEWS-OS 6.0.3

6.1/SONYP6176.doc       describes about patch SONYP6176 [lockd/statd]
```

```
6.1/SONYP6176.pch       patch for NEWS-OS 6.1

6.1.1/SONYP6207.doc     describes about patch SONYP6207 [lockd/statd]

6.1.1/SONYP6207.pch     patch for NEWS-OS 6.1.1
```

If you need further information, contact your dealer.

Sun Microsystems, Inc.

The following patches are now available to fix the vulnerabilities in rpc.statd. More details are in Sun Microsystems Security Bulletin #00135, dated May 21, 1996.

A. Solaris 2.x (SunOS 5.x) patches

Patches which replace the affected statd executable are available for every supported version of SunOS 5.x.

OS version	Patch ID
SunOS 5.3	102932-02
SunOS 5.4	102769-03
Sun0S 5.4_X86	102770-03
SunOS 5.5	103468-01
SunOS 5.5_X86	103469-01

B. Solaris 1.x (SunOS 4.1.x) patches

For SunOS 4.1.x, the fix is supplied in a new version of the "UFS file system and NFS locking" jumbo patch.

OS version	Patch ID
SunOS 4.1.3	100988-05
SunOS 4.1.3_U1	101592-07
SunOS 4.1.4	102516-04

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

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

```
File              BSD          SVR4        MD5
Name              Checksum     Checksum    Digital Signature
---------------   ----------   ---------   --------------------------
100988-05.tar.Z   10148 444     4116 888    ACE925E808A582D6CF9209FE7A51D23B
101592-07.tar.Z   21219 346     32757 692   7B7EE4BD5B2692249FDB9178746AA71B
102516-04.tar.Z   65418 201     61604 401   DB87F3DDA2F12FE2CFBB8B56874A1756
102769-03.tar.Z   38936 74      64202 148   9A8E4D9BE8C58FD532EE0E2140EF7F85
102770-03.tar.Z   04518 71      23051 141   F646E2B7AD66EEFBB32F6AB630796AF8
102932-02.tar.Z   34664 70      45816 139   66CB7F6AE48784A884BA658186268C41
103468-01.tar.Z   30917 82      46790 164   84680D9A0D2AEF62FFE1382C82684BE5
103469-01.tar.Z   31245 82      52288 164   F22AEB0FD91687DAB8ADC4DF10348DE8
```

The checksums shown above are from the BSD-based checksum (on 4.1.x, /bin/sum; on SunOS 5.x, /usr/ucb/sum) and from the SVR4 version on on SunOS 5.x (/usr/bin/sum).

Customers with Sun support contracts can obtain patches from:

- SunSolve Online
- Local Sun answer centers, worldwide
- SunSITEs worldwide

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

Customers without support contracts may now obtain security patches, "recommended" patches, and patch lists via SunSolve Online.

TGV/Cisco Systems, Inc.

Cisco MultiNet for OpenVMS is not vulnerable.

Appendix B: Example Workaround Scenario

The information given below was provided to the CERT/CC by Wolfgang Ley of DFN-CERT. It is reproduced here as an example of how to run the statd daemon as a user other than root on a Solaris system. This workaround may not be directly applicable on other vendor's systems, but an analogous solution may be possible. Please contact your vendor for assistance.

The statd daemon under Solaris 2.4 and 2.5 starts without problems if the following steps are taken.

1) Go into single user mode (ensure rpcbind and statd are not running)
2) Create a new user, e.g., "statd" with a separate uid/gid

3) Chown statd /var/statmon/* /var/statmon/*/*
4) Chgrp statd /var/statmon/* /var/statmon/*/*
5) Edit /etc/init.d/nfs.client startup script and change the start of the statd from:

```
/usr/lib/nfs/statd > /dev/console 2>&1
```

to:

```
/usr/bin/su - statd -c "/usr/lib/nfs/statd" >
/dev/console 2>&1
```

6) Reboot the system

The CERT Coordination Center thanks Andrew Gross of the San Diego Supercomputer Center for reporting this problem and Wolfgang Ley of DFN-CERT for his support in responding to this problem.

Revision History

Dec. 5, 1997 Appendix A - Added for NCR Corporation.

Sep. 24, 1997 Updated copyright statement

Nov. 12, 1996 Appendix A, SGI - replaced a URL with a pointer to updated information.

Sep. 18, 1996 Revised opening paragraph.

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

Appendix A, IBM - put a new URL in the "To Order" section.

Appendix A, Sun - removed a workaround for SunOS 4.x (patches now available).

Aug. 01, 1996 Appendix A, Hewlett-Packard - updated information.

July 26, 1996 Appendix A, NEC - added patch information.

July 5, 1996 Appendix A, Digital - added pointer to updated vendor information.

July 1, 1996 Appendix A, SGI - added pointer to release notes.

May 23, 1996 Appendix A, Sun - added pointer to patches.

May 10, 1996 Sec. I - added clarification about disabling rpc.lockd and rpc.statd.

Appendix A, TGV/Cisco Systems - added an entry.

Appendix A, Sun - added a workaround.

10 CA-1996-10: NIS+ Configuration Vulnerability

Original issue date: May 28, 1996
Last revised: October 20, 1997
Vendor information for Sun has been added to the UPDATES section.

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

The text of this advisory was originally released by the Australian Emergency Response Team on May 20, 1996, and updated on May 27, 1996, as AUSCERT advisory AA-96.02a.

Because of the seriousness of the problem, we are reprinting the AUSCERT advisory here with their permission. Only the contact information at the end has changed: AUSCERT contact information has been replaced with CERT/CC contact information.

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

AUSCERT has received information that a vulnerability exists under some configurations of NIS+. In vulnerable installations of NIS+, the access rights on the NIS+ passwd table are left in an unsecure state.

This vulnerability is known to exist in NIS+ installations initially created on Solaris 2.5 servers. Similar vulnerabilities in NIS+ configurations may also exist in previous versions of Solaris 2.

This vulnerability may allow any user with valid NIS+ credentials to gain root privileges.

AUSCERT recommends that any site which has NIS+ installed take this opportunity to check their installations and apply the appropriate workarounds as described in Section 3.

This updated advisory contains clarifications for sites requiring password aging facilities and sites running their NIS+ servers in NIS compatibility mode.

1. Description

NIS+ provides distributed network access to information sources such as password, group and host information. It maintains this information in the form of NIS+ tables. NIS+ tables contain the administrative information normally supplied by local files (such as /etc/passwd). As with the standard Unix administration files, setting secure permissions on the NIS+ tables is of utmost importance in maintaining system security.

NIS+ provides a comprehensive set of access rights for NIS+ tables. This includes permissions not only on NIS+ tables but also individual columns and entries in those tables. Due to the added

complexity, sites need to be particularly diligent in ensuring that permissions on NIS+ tables (and associated entries and columns) are secure.

AUSCERT encourages sites running NIS+ to gain a good understanding of the permission model used by NIS+. A complete description may be found in the NIS+ documentation set. The rest of this advisory assumes a good understanding of NIS+ permission controls.

AUSCERT has received information that under some installations of NIS+ the permissions on the NIS+ passwd table are left in an unsecure state.

This vulnerability is known to exist in NIS+ installations initially created on Solaris 2.5 servers. Similar vulnerabilities in NIS+ configurations may also exist in previous versions of Solaris 2.

2. Impact

Any user with login access to a client or server that uses NIS+ for authentication may gain root privileges.

3. Workarounds

NIS+ uses an access control mechanism for granting access to NIS+ tables which is similar (but not identical) to that used by the standard Unix file system. NIS+ tables are assigned permissions for the NIS+ user categories nobody, owner, group and world. NIS+ also has permissions associated with columns and individual entries in NIS+ tables.

Under some installations of NIS+ the permissions of the NIS+ passwd table and its columns are left in an unsecure state. These permissions can be viewed using niscat(1).

To check the permissions on the NIS+ passwd table, sites can use:

```
# niscat -o passwd.org_dir
```

This should produce output similar to:

```
Object Name   : passwd
Owner         : myhost.mydomain.org.
Group         : admin.mydomain.org.
Domain        : org_dir.mydomain.org.
Access Rights : ----rmcdrmcd----
Time to Live  : 12:0:0
Object Type   : TABLE
Table Type          : passwd_tbl
Number of Columns   : 8
Character Separator : :
Search Path         :
Columns             :
        [0]     Name          : name
```

```
                Attributes    : (SEARCHABLE, TEXTUAL DATA, CASE
SENSITIVE)
                Access Rights : r---------------
        [1]     Name          : passwd
                Attributes    : (TEXTUAL DATA)
                Access Rights : -----m----------
        [2]     Name          : uid
                Attributes    : (SEARCHABLE, TEXTUAL DATA, CASE
SENSITIVE)
                Access Rights : r---------------
        [3]     Name          : gid
                Attributes    : (TEXTUAL DATA)
                Access Rights : r---------------
        [4]     Name          : gcos
                Attributes    : (TEXTUAL DATA)
                Access Rights : r---------------
        [5]     Name          : home
                Attributes    : (TEXTUAL DATA)
                Access Rights : r---------------
        [6]     Name          : shell
                Attributes    : (TEXTUAL DATA)
                Access Rights : r---------------
        [7]     Name          : shadow
                Attributes    : (TEXTUAL DATA)
                Access Rights : ----------------
```

This output shows two types of access rights associated with the NIS+ passwd table. First, the default access rights for the table, which are given at the start of the output (----rmcdrmcd----). Second, the access rights associated with each column.

In particular, sites should check the access rights on the columns of the NIS+ passwd table. It should be noted that it appears that individual entries of the passwd table are owned by individual users. The above access rights do not allow a user to modify any part of their passwd table entry besides their own passwd field. For many environments this is acceptable.

However, depending on the local site configuration and requirements, additional access rights may also be needed.

- Sites that wish users to be able to change their shell or gcos information may have the (m)odify bit set for owner on the shell or gcos column as needed.
- Sites that have their NIS+ servers running in NIS compatibility mode to serve NIS clients may require (r)ead permission for nobody on the NIS+ passwd table.
- Sites that are using password aging may require additional access rights on the shadow column. The exact access rights will depend on the particular NIS+ version (including patches). Sites are encouraged to check their local documentation for more information.

Other than this, the access rights on columns should appear as shown in the niscat(1) output above.

Any additional access rights on the table or its columns besides those shown above may allow a user to gain additional privileges, including possibly root. Sites should completely understand the ramifications if they allow additional access rights.

Sites may set the access rights on the NIS+ passwd table, as shown in the above output, by issuing the following commands as root on the master NIS+ server.

To set the default access rights for the NIS+ passwd table:

```
# nischmod na-rmcd,og+rmcd passwd.org_dir
```

To set the column access rights on the NIS+ passwd table:

```
# nistbladm -u name=na-rmcd,n=r passwd.org_dir
# nistbladm -u passwd=na-rmcd,o=m passwd.org_dir
# nistbladm -u uid=na-rmcd,n=r passwd.org_dir
# nistbladm -u gid=na-rmcd,n=r passwd.org_dir
# nistbladm -u gcos=na-rmcd,n=r passwd.org_dir
# nistbladm -u home=na-rmcd,n=r passwd.org_dir
# nistbladm -u shell=na-rmcd,n=r passwd.org_dir
# nistbladm -u shadow=na-rmcd passwd.org_dir
```

After making any changes in access rights, AUSCERT recommends that sites verify the changes they have made using niscat(1), as shown previously.

Sites that have replica NIS+ servers may use nisping(1m) to propagate the changes to the replica servers in a timely manner.

4. Additional measures

AUSCERT recommends that sites take this opportunity to ensure that all NIS+ tables have access rights in accordance with the local site security policy. This also includes checking access rights on all the columns and entries of the NIS+ tables in addition to the default access rights of the tables themselves.

AUSCERT wishes to thank Ivan Angus and David Clarke of ANU for reporting this vulnerability and for their advice in the preparation of this advisory. AUSCERT also acknowledges Marek Krawus of UQ, Reinhard Uebel and Mark McPherson of QTAC for their assistance.

AUSCERT takes no responsibility for the consequences of applying the contents of this document.

UPDATES

CERT/CC received information concerning an additional problem with the ROW access rights in the NIS+ password table. Accounts created on Solaris 2.4 and 2.5 systems have excessive rights on the system. These new super accounts have read, modify, create, and delete access rights on their own rows in the nisplus password table. This means they can alter all attributes on their own entries.

To determine if your system is so affected, execute the following:

```
% niscat -o '[name=juke],passwd.org_dir' | egrep "Access"
```

If the output displays information similar to the following:

```
Access Rights : ----rmcdr---r---
                    ^^^^
```

then the owner can read, modify, change, and delete information.

The rights at this level should be more restrictive, and the individual rights on entries should be less restrictive. The less restrictive rights on entries allow a user to change their password entry, the GECOS field, and even the shell depending upon how the entry rights are set.

The output from the niscat above should look like the following:

```
Access Rights : ----r-----------
```

This allows only the user to read information from the password table.

One way to determine which entries in the password table need to be changed is the following:

```
% niscat -o '[ ],passwd.org_dir' | egrep "Owner|rmc"
```

To fix the entries, use the following:

```
% nischmod o=r,ngw-rmdc '[ ],passwd.org_dir'
```

This sets the owner permissions to r (read) and removes all permissions from nobody, group, and world.

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.

Sun Microsystems, Inc.

Sun Microsystems has provided the following list of patches in response to this advisory:

103266-01 5.5
103267-01 5.5_x86
103270-01 5.4
103271-01 5.4_x86
103269-01 5.3

Revision History

```
Oct. 27, 1997  Vendor information for Sun has been added to the
UPDATES section.

Sep. 24, 1997  Updated copyright statement

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

Beginning of the advisory - removed AUSCERT advisory header to avoid
confusion.

June 12, 1996  Updates section - added clarification concerning ROW
access rights.
```

11 CA-1996-11: Interpreters in CGI bin Directories

Original issue date: May 29, 1996
Last revised: September 24, 1997
Updated copyright statement

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

Many sites that maintain a Web server support CGI programs. Often these programs are scripts that are run by general-purpose interpreters, such as /bin/sh or PERL. If the interpreters are located in the CGI bin directory along with the associated scripts, intruders can access the interpreters directly and arrange to execute arbitrary commands on the Web server system. This problem has been widely discussed in several forums. Unfortunately, some sites have not corrected it.

The CERT Coordination Center recommends that you never put interpreters in a Web server's CGI bin directory.

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

I. Description

To execute CGI scripts, a Web server must be able to access the interpreter used for that script. Early documentation for Netscape and other servers recommended placing the interpreters in the CGI bin directory to ensure that they were available to run the script.

All programs in the CGI bin directory can be executed with arbitrary arguments, so it is important to carefully design the programs to permit only the intended actions regardless of what arguments are used. This is difficult enough in general, but is a special problem for general-purpose interpreters since they are designed to execute arbitrary programs based on their arguments. *All* programs in the CGI bin directory must be evaluated carefully, even relatively limited programs such as gnu-tar and find.

Note that the directory for CGI programs is typically called "cgi-bin" but the server may be configured to use a different name.

II. Impact

If general-purpose interpreters are accessible in a Web server's CGI bin directory, then a remote user can execute any command the interpreters can execute on that server.

III. Solution

The solution to this problem is to ensure that the CGI bin directory does not include any general-purpose interpreters, for example

PERL
Tcl
UNIX shells (sh, csh, ksh, etc.)

A variety of methods can be used to safely install such interpreters; methods vary depending on the system and Web server involved.

On Unix systems, the location of the interpreter is given on the first line of the script:

#! /path/to/interpreter

On other systems, such as NT, there is an association between filename extensions and the applications used to run them. If your Web server uses this association, you can give CGI scripts an appropriate suffix (for example, ".pl" for PERL), which is registered to the appropriate interpreter. This avoids the need to install the interpreter in the CGI bin directory, thus avoiding the problem.

Check with your Web server vendor for specific information.

Netscape reports that the 2.0 versions of their FastTrack and Enterprise Servers, (both the current Beta and upcoming final versions), do support file interpreter associations.

Further reading:

Tom Christiansen has a Web page with details about this problem and a script that can be used to test for it: http://perl.com/perl/news/latro-announce.html.

Lincoln Stein's WWW Security FAQ includes a section on "Problems with Specific Servers," which discusses this and related problems:
http://www.genome.wi.mit.edu/WWW/faqs/www-security-faq.html.

The CERT Coordination Center thanks Lincoln Stein, Tom Christiansen, and the members of AUSCERT and DFN-CERT for their contributions to the information in this advisory.

Revision History

Sep. 24, 1997 Updated copyright statement

Aug. 30, 1996 Removed references to CA-96.11.README.

12 CA-1996-12: Vulnerability in suidperl

Original issue date: June 26, 1996
Last revised: September 24, 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 systems that contain the suidperl program and that support saved set-user-ID and saved set-group-ID. By exploiting this vulnerability, anyone with access to an account on such a system may gain root access.

Saved set-user-IDs and set-group-IDs are sometimes referred to as POSIX saved IDs. suidperl is also known as sperl followed by a version number, as in sperl5.002.

Perl versions 4 and 5 can be compiled and installed in such a way that they will be vulnerable on some systems. If you have installed the suidperl or sperl programs on a system that supports saved set-user-ID and set-group-ID, you may be at risk.

The CERT Coordination Center recommends that you first disable the suidperl and sperl programs (Section III.A). If you need the functionality, we further recommend that you either apply a patch for this problem or install Perl version 5.003 (Section III.B). If neither a patch nor a new version are viable alternatives, we recommend installing the wrapper written by Larry Wall as a workaround for this problem (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

On some systems, setuid and setgid scripts (scripts written in the C shell, Bourne shell, or Perl, for example, with the set user or group ID permissions enabled) are insecure due to a race condition in the kernel. For those systems, Perl versions 4 and 5 attempt to work around this vulnerability with a special program named suidperl, also known as sperl. Even on systems that do provide a secure mechanism for setuid and setgid scripts, suidperl may also be installed--although it is not needed.

suidperl attempts to emulate the set-user-ID and set-group-ID features of the kernel. Depending on whether the script is set-user-ID, set-group-ID, or both, suidperl achieves this emulation by first changing its effective user or group ID to that of the original Perl script. suidperl then reads and executes the script as that effective user or group. To do these user and group ID changes correctly, suidperl must be installed as set-user-ID root.

On systems that support saved set-user-ID and set-group-ID, suidperl does not properly relinquish its root privileges when changing its effective user and group IDs.

II. Impact

On a system that has the suidperl or sperl program installed and that supports saved set-user-ID and saved set-group-ID, anyone with access to an account on the system can gain root access.

III. Solution

The command in Section A helps you determine if your system is vulnerable and, if it is, optionally disables the suidperl and sperl programs that it locates. After you have run this command on all of your systems, your system will no longer be vulnerable.

If you find that your system is vulnerable, then you need to replace the suidperl and sperl programs with new versions. Section B describes how to do that.

Finally, Section C identifies a wrapper that can be used in place of the suidperl program.

A. How to determine if your system is vulnerable

To determine if a system is vulnerable to this problem and to disable the programs that are believed to be vulnerable, use the following find command or a variant. Consult your local system documentation to determine how to tailor the find program on your system.

You will need to run the find command on each system you maintain because the command examines files on the local disk only. Substitute the names of your local file systems for FILE_SYSTEM_NAMES in the example. Example local file system names are /, /usr, and /var. You must do this as root.

Note that this is one long command, though we have separated it onto three lines using backslashes.

```
find FILE_SYSTEM_NAMES -xdev -type f -user root \

          \( -name 'sperl[0-9].[0-9][0-9][0-9]'-o -name \

          'suidperl' \) -perm -04000 -print -ok chmod ug-s '{}' \;
```

This command will find all files on a system that are

- only in the file system you name (FILE_SYSTEM_NAMES -xdev) - regular files (-type f)
- owned by root (-user root)
- named appropriately (-name 'sperl[0-9].[0-9][0-9][0-9]' -o -name 'suidperl')
- setuid root (-perm -04000)

Once found, those files will

- have their names printed (-print)
- have their modes changed, but only if you type `y' in response to the prompt (-ok chown ug-s '{}' \;)

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

Vendor patches

You may be vulnerable if your vendor supports saved set-user-ID and set-group-ID and ships suidperl or sperl. You need to get a patched version from your vendor. Appendix A contains information provided by the following vendors. If you vendor is not on this list, please contact the vendor directly.

Vendor or Source

Apple Computer, Inc.
Data General Corp.
Digital Equipment Corp.
FreeBSD, Inc.
Hewlett-Packard Company
IBM Corporation
Linux
NEC
Open Software Foundation
Sony Corporation
X.org

Until you can install a patch, we recommend disabling suidperl. The find command above will help you do that. If you need suidperl or sperl, an alternative is to install the wrapper described in Section C.

Source code patches

If you have installed Perl from source code, you should install source code patches. Patches are available from the CPAN (Comprehensive Perl Archive Network) archives.

Patch for Perl Version 4:

File	src/fixsuid4-0.pat
MD5 Checksum	af3e3c40bbaafce134714f1381722496

Patch for Perl Version 5:

File	src/fixsuid5-0.pat
MD5 Checksum	af3e3c40bbaafce134714f1381722496

In addition, Perl version 5.003 contains this patch, so installing it on your system also addresses this vulnerability. Perl 5.003 is available from the CPAN archives. Here are the specifics:

File	src/5.0/perl5.003.tar.gz
MD5 Checksum	b1bb23995cd25e5b750585bfede0e8a5

The CPAN archives can be found at the following locations:

CPAN master site
ftp://ftp.funet.fi/pub/languages/perl/CPAN/.

Africa
ftp://ftp.is.co.za/programming/perl/CPAN/

Asia
ftp://dongpo.math.ncu.edu.tw/perl/CPAN/ ftp://ftp.lab.kdd.co.jp/lang/perl/CPAN/

Australasia
ftp://coombs.anu.edu.au/pub/perl/
ftp://ftp.mame.mu.oz.au/pub/perl/CPAN/
ftp://ftp.tekotago.ac.nz/pub/perl/CPAN/

Europe
ftp://ftp.arnes.si/software/perl/CPAN/
ftp://ftp.ci.uminho.pt/pub/lang/perl/
ftp://ftp.cs.ruu.nl/pub/PERL/CPAN/
ftp://ftp.demon.co.uk/pub/mirrors/perl/CPAN/
ftp://ftp.funet.fi/pub/languages/perl/CPAN/
ftp://ftp.ibp.fr/pub/perl/CPAN/ ftp://ftp.leo.org/pub/comp/programming/languages/perl/CPAN/
ftp://ftp.pasteur.fr/pub/computing/unix/perl/CPAN/
ftp://ftp.rz.ruhr-uni-bochum.de/pub/programming/languages/perl/CPAN/
ftp://ftp.sunet.se/pub/lang/perl/CPAN/
ftp://ftp.switch.ch/mirror/CPAN/
ftp://unix.hensa.ac.uk/mirrors/perl-CPAN/

North America
ftp://ftp.cis.ufl.edu/pub/perl/CPAN/
ftp://ftp.delphi.com/pub/mirrors/packages/perl/CPAN/

ftp://ftp.sedl.org/pub/mirrors/CPAN/
ftp://ftp.sterling.com/programming/languages/perl/
ftp://ftp.uoknor.edu/mirrors/CPAN/
ftp://uiarchive.cso.uiuc.edu/pub/lang/perl/CPAN/

C. If you need setuid or setgid Perl scripts and are unable to apply the source code patches listed in Section B,

we suggest that you retrieve Larry Wall's fixsperl script noted below. fixsperl is a script that replaces the suidperl and sperl programs with a wrapper that eliminates the vulnerability. The script is available from the CPAN archives as

File	src/fixsperl-0
MD5 Checksum	f13900d122a904a8453a0af4c1bdddc6

Note that this script should be run one time, naming every suidperl or sperl file on your system. If you add another version of suidperl or sperl to your system, then you must run fixsperl on those newly installed versions.

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.

Apple Computer, Inc.

A/UX 3.1.1 and earlier support saved set-{user,group}-ids.

A/UX 3.1.1 and earlier do not have Perl as part of the standard product.

Data General Corporation

Data General does support saved set-user-IDs and set-group-IDs on DG/UX.

Data General does not ship suidperl or sperl* with DG/UX.

Digital Equipment Corporation

Digital UNIX and Digital's ULTRIX Operating systems do support saved suid and saved guid in the process context.

Digital does not ship Perl with any operating system.

FreeBSD, Inc.

This information is taken from FreeBSD advisory SA-96:12.

For the complete text of the advisory, please refer to
ftp://freebsd.org/pub/CERT/patches/SA-96:12/.

This vulnerability is present on all systems with the
_POSIX_SAVED_IDS functionality extension where suidperl has been installed.

One may disable the setuid bit on all copies of the setuid version of perl. This will close the vulnerability but render inoperable setuid perl scripts. No software currently shipping as part of FreeBSD relies on this functionality so the impact is only to third party software.

As root, execute the commands:

```
# chmod 111 /usr/bin/suidperl
# chmod 111 /usr/bin/sperl4.036
```

In addition, if you have installed the perl5 port:

```
# chmod 111 /usr/local/bin/suidperl
# chmod 111 /usr/local/bin/sperl5.001
```

then verify that the setuid permissions of the files have been removed. The permissions array should read "-r-xr-xr-x" as shown here:

```
# ls -l /usr/bin/s*perl*

---x--x--x  2 root bin 307200  Jun 1 17:16  /usr/bin/sperl4.036

---x--x--x  2 root bin 307200  Jun 1 17:16  /usr/bin/suidperl
```

and for the perl5 port:

```
# ls -l /usr/local/bin/s*perl*

---x--x--x 2 rootbin 397312 Jan 22 15:15 /usr/local/bin/sperl5.001

---x--x--x 2 rootbin 397312 Jan 22 15:15 /usr/local/bin/suidperl
```

Other information:

NOTE A patch for perl is available directly from Larry Wall (the author of perl) which solves this vulnerability in a different fashion than the FreeBSD patches. You may apply either the

FreeBSD patches, or Larry's patches, or both. The patches solve the problem via two different mechanisms.

Patches are available which eliminate this vulnerability. The following patch should be applied to the system sources and suidperl should be rebuilt and reinstalled.

Apply the patch, then:

- cd /usr/src/gnu/usr.bin/perl/sperl
- make depend
- make all
- make install

A similar patch is also available for the perl5 port. Apply the following patch by moving it into the patch directory for the port distribution and rebuilding and installing perl5:

- cd /usr/ports/lang/perl5
- cp <location of new patches>/patch-a[ab] patches
- make all
- make install

NOTE: These patches do NOT solve the vulnerability for FreeBSD 2.0 or 2.0.5. These only solve the problem for 2.1 and later. Patches specific to FreeBSD 2.0 and 2.0.5 are available at the URL listed above.

Hewlett-Packard Company

HP/UX versions 8.X, 9.X, and 10.X all support saved set-user-id.

None of HP/UX versions 8.X, 9.X, and 10.X have Perl as part of the standard product.

IBM Corporation

AIX versions 3.2.5 and 4.X support saved set-user-id.

AIX versions 3.2.5 and 4.X do not have Perl as part of the standard product. However, the SP2's PSSP software does contain suidperl, but the program is not installed with the setuid bit set.

Linux

Linux 1.2 and 2.0 support saved set-user-id.

Most distributions of Linux provide suidperl and sperl.

The fixsperl script works on linux, and it is recommended that this fix be applied until a new Perl release is made.

NEC

OS	Support Saved Sets?	Provide suidperl?
UX/4800	yes	no
EWS-UX/V (Rel4.2MP)	yes	no
UP-UX/V (Rel4.2MP)	yes	no
EWS-UX/V (Rel4.2)	yes	no

Open Software Foundation

OSF/1 1.3 or later support saved set-user-id

OSF/1 1.3 or later does not have Perl as part of the standard product.

Sony Corporation

NEWS-OS 4.X does not support saved set-user-id and therefore any version of Perl on that system is not vulnerable.

NEWS-OS 6.X does support saved set-user-id.

X.org

None of X.org's development systems are vulnerable to the saved set-user-IDs and set-group-IDs problems, and suidperl is not shipped with either of our products.

The CERT Coordination Center staff thanks Paul Traina, Larry Wall, Eric Allman, Tom Christiansen, and AUSCERT for their support in the development of this advisory.

Revision History

```
Sep. 24, 1997 Updated copyright statement

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

July 01, 1996 Appendix, FreeBSD - added an entry for this vendor.

June 27, 1996 Appendix, NEC - added an entry for this vendor.

June 26, 1996 Appendix, Digital - added an entry for this vendor.
```

13 CA-1996-13: Vulnerability in the dip program

Original issue date: July 9, 1996
Last revised: September 24, 1997
Updated copyright statement

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

The CERT Coordination Center has received several reports of exploitations of a vulnerability in the dip program on Linux systems. The dip program is shipped with most versions of the Linux system; and versions up to and including version 3.3.7n are vulnerable. An exploitation script for Linux running on X86-based hardware is publicly available. Although exploitation scripts for other architectures and operating systems have not yet been found, we believe that they could be easily developed.

The CERT Coordination Center recommends that you disable dip and re-enable it only after you have installed a new version. Section III below describes how to do that.

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

I. Description

dip is a freely available program that is included in most distributions of Linux. It is possible to build it for and use it on other UNIX systems.

The dip program manages the connections needed for dial-up links such as SLIP and PPP. It can handle both incoming and outgoing connections. To gain access to resources it needs to establish these IP connections, the dip program must be installed as set-user-id root.

A vulnerability in dip makes it possible to overflow an internal buffer whose value is under the control of the user of the dip program. If this buffer is overflowed with the appropriate data, a program such as a shell can be started. This program then runs with root permissions on the local machine.

Exploitation scripts for dip have been found running on Linux systems for X86 hardware. Although exploitation scripts for other architectures and operating systems have not yet been found, we believe that they could be easily developed.

II. Impact

On a system that has dip installed as set-user-id root, anyone with access to an account on that system can gain root access.

III. Solution

Follow the steps in Section A to disable your currently installed version of dip. Then, if you need the functionality that dip provides, follow the steps given in Section B.

A. Disable the presently installed version of dip.

As root,

chmod 0755 /usr/sbin/dip

By default, dip is installed in the /usr/sbin directory. Note that it may be installed elsewhere on your system.

B. Install a new version of dip.

If you need the functionality that dip provides, retrieve and install the following version of the source code for dip, which fixes this vulnerability. dip is available from

ftp://sunsite.unc.edu/pub/Linux/system/Network/serial/dip/dip337o-uri.tgz
ftp://sunsite.unc.edu/pub/Linux/system/Network/serial/dip/dip337o-uri.tgz.sig

MD5 (dip337o-uri.tgz) = 45fc2a9abbcb3892648933cadf7ba090

SHash (dip337o-uri.tgz) = 6e3848b9b5f9d5b308bbac104eaf858be4dc51dc

---

The CERT Coordination Center staff thanks Uri Blumenthal for his solution to the problem and Linux for their support in the development of this advisory.

Revision History

Sep. 24, 1997 Updated copyright statement

Aug. 30, 1996 Removed references to CA-96.13.README.

14 CA-1996-14: Vulnerability in rdist

Original issue date: July 24, 1996
Last revised: January 15, 1998
Updated information for NCR.

A complete revision history is at the end of this file. **This advisory supersedes CA-91.20 and CA-94.04.**

The CERT Coordination Center has received reports that a new vulnerability in rdist has been found and an exploitation script is widely available. Current reports indicate that the script works on x86-based versions of the UNIX Operating System; however, we believe that it would not be difficult to write variants that work on other instruction sets and configurations.

The CERT/CC Staff recommends following the steps in Section III.A. to determine if your system is vulnerable and to disable vulnerable programs, then following your vendor's instructions (Section III.B and Appendix A). Until you can install a vendor patch, you may want to install a freely available version of rdist, noted in 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

The rdist program is a UNIX Operating System utility used to distribute files from one host to another. On most systems, rdist is installed as set-user-id root, a necessity due to its design. Unfortunately, this setting makes it a favorite target for vulnerability investigation.

A new vulnerability in rdist has been discovered and reported. The vulnerability lies in the lookup() subroutine where the value of a command line argument is used to overflow the subroutine call stack. If that argument is specially crafted with native machine code, lookup() returns control to the code added to the call stack instead of the subroutine that called lookup(). If, for example, this added code uses a member of the exec system call family and names /bin/sh as the program to be executed, that shell is then run with set-user-id root privileges. No matter what code is added, the code runs with set-user-id root privileges.

An exploitation program, which is circulating on the Internet, takes advantage of this vulnerability. While it purports to work only on x86-based versions of the UNIX Operating System, variants tuned to other instruction sets and configurations are straightforward to write.

II. Impact

On unpatched systems, anyone with access to a local account can gain root access.

III. Solution

We urge you to follow the steps in Section A to determine if your system is potentially vulnerable and, if it is, to turn off rdist while you decide how to proceed. If you need the functionality that rdist provides, install a vendor patch (Sec. B). Until you can do so, you may want to install a freely available version of rdist that does not need to be installed as set-user-id root and is, therefore, not susceptible to the exploitation described in this advisory (Sec. C).

A. How to determine if your system is vulnerable

To determine if a system is vulnerable and to disable the programs that are believed to be vulnerable, use the following find command or a variant. Consult your local system documentation to determine how to tailor the find program on your system.

You will need to run the find command on each system you maintain because the command examines files on the local disk only. Substitute the names of your local file systems for FILE_SYSTEM_NAMES in the example. Example local file system names are /, /usr, and /var. You must do this as root.

Note that this is one long command, though we have separated it onto two lines using a backslash.

```
find FILE_SYSTEM_NAMES -xdev -type f -user root \
        -name rdist -perm -04000 -print -ok chmod u-s '{}' \;
```

This command will find all files on a system that are only in the file system you name (FILE_SYSTEM_NAMES -xdev)

- regular files (-type f)
- owned by root (-user root)
- named rdist
- setuid (-perm -04000)

Once found, those files will have their names printed (-print)

- have the setuid mode removed, but only if you type `y' in response to the prompt (-ok chmod u-s '{}' \;)

B. Obtain and install the appropriate patch

Below is a list of vendors who have provided information. Details are in Appendix A of this advisory. We will update the advisory as we receive more information.

Berkeley Software Design, Inc.
Data General Corporation
Digital Equipment Corporation
FreeBSD, Inc.
Hewlett-Packard Company
IBM Corporation

Linux
NEC Corporation
NCR Corporation
The Santa Cruz Operation
Sequent Computer Systems
Silicon Graphics, Inc.
Sun Microsystems, Inc.

If your vendor's name is not on this list, please contact the vendor directly.

C. If you need the functionality that rdist provides but a patched version is not yet available from your vendor:

Consider installing rdist-6.1.3, which is freely available from
ftp://usc.edu/pub/rdist/rdist-6.1.3.tar.gz.

MD5 (rdist-6.1.3.tar.gz) = 8a76b880b023c5e648b7cb77b9608b9f

The README file in the distribution explains how to configure and install this version of rdist.

We strongly recommend that you configure this version of rdist to use rsh instead of rcmd. Here is the relevant text from the README:

By default rdist uses *rsh(1c)* to make connections to remote hosts. This has the advantage that rdist does not need to be setuid to "root". This eliminates most potential security holes. It has the disadvantage that it takes slightly more time for rdist to connect to a remote host due to the added overhead of doing a fork() and then running the *rsh(1c)* command.

For versions of rdist V6 prior to 6.1.3: If you compile rdist with -DDIRECT_RCMD *and* you run rdist setuid to root, you are vulnerable to the problem described in this advisory. You need to update to rdist version 6.1.3.

Note that by default, rdist V6 is distributed to compile without -DDIRECT_RCMD and not run setuid to root. If you have previously built version 6.X of rdist with the -DDIRECT_RCMD directive added to the $(DEFS_LOCAL) and set "RDIST_MODE = 4555" in "Makefile.local", we recommend that you first disable this version with the find command given in Section III.A above, then either rebuild rdist with its default settings or upgrade to 6.1.3.

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.

Berkeley Software Design, Inc.

BSD/OS is vulnerable to this problem.

BSDI has released a patch for rdist in BSD/OS V2.1.

Sites using the non-kerberized rdist should install patch U210-018, which is available from the patches@bsdi.com mailback server and also from
ftp://ftp.bsdi.com/bsdi/patches/patches-2.1/U210-018

md5 checksum: 86005d8bbb67eb737120741bd254d26a U210-018

Domestic licensees that are using the Kerberos package should install patch D210-018 from: patches@bsdi.com mailback server (this patch is available only to domestic licensees because of US export restrictions on crypto software). Be sure to install only the appropriate patch.

md5 checksum: b2060ec4eb9b18ace4e76bcb9441353f D210-018

Data General Corporation

Data General does not provide a version of rdist as part of the standard release of DG/UX. Rdist is available as contributed software which is not supported by Data General. This problem will be fixed in the next release of the contributed software package.

Digital Equipment Corporation

#96.0329A

SOURCE:

Digital Equipment Corporation
Software Security Response Team

SUMMARY PATCH-ID INFORMATION:
The rdist patch-id's identified in this advisory will not be applicable to versions previous to those identified in the OP/SYS identified for each patch.

NOTE

1. These patch's must be applied if an update or installation is performed thru V3.2c of Digital UNIX
2. The solutions have been included in releases of Digital UNIX after V3.2c

TITLES

```
OSF_V2_0      (Patch ID: OSFV20-244-1>

OSF_V3_0      (Patch ID: OSF300-242)

OSF_V3_0B     (Patch ID: OSF305-300242)

OSF_V3_2      (Patch ID: OSF320-184)
```

```
OSF_V3_2B     (Patch ID: OSF325-320184)

OSF_V3_2C     (Patch ID: OSF350-061)
```

PATCH AVAILABILITY:

Software service contract or warranty customers may obtain the patched rdist through normal Digital support channels, via AES (Advanced Electronic Services). These patch's are available from the remedial patch stream for the versions identified above and may be found in the applicable versions readme files.

ftp://ftp.service.digital.com/public/osf

Please refer to applicable Release Note information prior to upgrading your installation.

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

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.

- DIGITAL EQUIPMENT CORPORATION
7/23/96

FreeBSD, Inc.

Versions affected:

FreeBSD 2.0, 2.0.5, 2.1, 2.1-stable, and 2.2-current

Versions corrected:

2.1-stable and 2.2-current as of 1996-07-11

Workaround:

As root, execute the commands:

```
# chflags noschg /usr/bin/rdist
# chmod u-s,go-rx /usr/bin/rdist
```

Patches: ftp://freebsd.org/pub/CERT/patches/SA-96:16/

For more information: ftp://freebsd.org/pub/CERT/advisories/SA-96:16/

Hewlett-Packard Company

The rdist vulnerability can be eliminated from releases 10.0, 10.01, 10.10, and 10.20 of HP-UX by applying the patches mentioned below. HP-UX releases prior to 10.X and after 10.20 (i.e., 10.30) are not vulnerable. HP/UX 9.X is not vulnerable.

Apply patches PHNE_8107	(series 700/800, HP-UX 10.00 & 10.01)
and PHCO_7798	(series 700/800, HP_UX 10.00 & 10.01)
or patch PHNE_7919	(series 700/800, HP-UX 10.10)
PHNE_7920	(series 700/800, HP-UX 10.20)

All patches are available now, except PHNE_7920 which will be available after 8 August.

See HEWLETT-PACKARD SECURITY BULLETIN: HPSBUX9608-036, 08 Aug 96 for more details.

IBM Corporation

AIX is vulnerable to this problem. Fixes are in process but are not yet available. The APAR numbers for the fixes are given below. In the meantime, we recommend removing the setuid bit from the /usr/bin/rdist program.

To remove the setuid bit, follow these instructions.

As the root user, type:

chmod u-s /usr/bin/rdist

AIX 3.2

Apply the following fix to your system:

APAR - IX59741

AIX 4.1

Apply the following fix to your system:

APAR - IX59742

To determine if you have this APAR on your system, run the following command:

instfix -ik IX59742

AIX 4.2

Apply the following fix to your system:

APAR - IX59743

To determine if you have this APAR on your system, run the following command:

instfix -ik IX59743

To Order

APARs may be ordered using FixDist or from the IBM Support Center. For more information on FixDist, reference URL: http://service.software.ibm.com/aixsupport/ or send e-mail to aixserv@austin.ibm.com with a subject of "FixDist".

IBM and AIX are registered trademarks of International Business Machines Corporation.

Linux

Almost all Linux distributions ship with rdist non setuid. If you have changed your rdist to run setuid you are probably vulnerable.

NEC Corporation

EWS-UX/V(Rel4.2)	not vulnerable
EWS-UX/V(Rel4.2MP)	not vulnerable
UP-UX/V(Rel4.2MP)	not vulnerable
UX/4800	not vulnerable

NCR Corporation

NCR is delivering a set of operating system dependent patches which contain an update for this problem . Accompanying each patch is a README file which discusses the general purpose of the patch and describes how to apply it to your system.

Recommended solution:
Apply one of the following patches depending on the revision of the inet package installed on your system. To check its version execute:

pkginfo -x inet

For inet 5.01.xx.xx: - PINET501 (Version later than 05.01.01.59)
For inet 6.01.xx.xx: - PINET601 (Version later than 06.01.00.19)
For inet 6.01.xx.xx: - PINET601 (Version later than 06.02.00.01)

The Santa Cruz Operation

The following releases of SCO Software are known to contain a version of rdist that is vulnerable:

SCO OpenServer 5.0.2, 5.0.0
SCO Internet FastStart 1.0

SCO Open Server Enterprise/Network System 2.0, 3.0
SCO Open Desktop 2.0, 3.0
SCO Open Desktop Lite 3.0

SCO UnixWare 2.0, 2.1

SCO TCP/IP 1.2.0, 1.2.1

Patches are being developed for the following releases:

SCO OpenServer 5.0.2, 5.0.0
SCO Internet FastStart 1.0
SCO UnixWare 2.1

Sequent Computer Systems

Sequent systems do not ship with rdist.

Silicon Graphics, Inc.

All SGI IRIX versions of rdist are not vulnerable.

No action is required.

(When using the find command on SGI IRIX systems, use -mount instead of - -xdev. The latter is not supported on SGI IRIX systems.)

Sun Microsystems, Inc.

The following patches correct the rdist vulnerability (Sun bug id 1258139), described in this advisory, on systems running Solaris 1.x or 2.x.

Architecture	SunOS	Solaris	Patch	MD5 checksum for rdist binary
SPARC	4.1.3	1.1	100383-07	5F2C2B782881FE18D2737B5FA0AEC489
	4.1.3_U1	1.1.1	103823-01	B330358F4E66CD544B9B60AF453C5F2B
	4.1.4	1.1.2	103824-02	419369cc4b3514a9c12b4cdac207fde7
	5.3	2.3	101494-02	1DD34E9E7C50B2C863E30D67DFD1A905
	5.4	2.4	103813-01	90DD81A4C32F7D583737F171B821386B
	5.5	2.5	103815-01	C3BBE3F6758B0BBA7D45CB05009ED80E
	5.5.1	2.5.1	103817-01	89735351119896FEB7469DCA76788561
X86	5.4	2.4	103814-01	EE4509D9CF87DBD29ABB7A72C8330F89

	5.5	2.5	103816-01	3363670F316A06803ECCDD9FFAE95126
	5.5.1	2.5.1	103818-01	8C2E8CFDE7A2AE6D5EC89139D592E71C
PowerPC	5.5.1	2.5.1	103819-01	C3FC0E54B23E4209496A4735D09DFFEF

These patches will be available through your local SunService and SunSoft Support Services organizations by 9:00 PDT Wednesday, July 24. They will also be available at the same time from SunSolve Online, via the URL http://sunsolve1.sun.com.

The CERT Coordination Center staff thanks Michael Cooper (Michael.Cooper@Sun.Com) for his work on resolving this problem. He is the maintainer of the publicly available version of rdist.

Revision History

Jan. 15, 1998 Updated vendor information for NCR.

Sep. 24, 1997 Updated copyright statement

Nov. 27, 1996 Appendix A, Sun - updated patch information for Solaris 1.1.2, SunOS 4.1.4.

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

Aug. 22, 1996 Appendix A, SGI - added note about using the find command.

Aug. 12, 1996 Appendix A, Hewlett-Packard - modified the entry.

July 30, 1996 Solution Section III.A - corrected two misprints in the results of the find command.

July 24, 1996 Appendix A, Digital - added information.
IBM - put a new URL in the "To Order" section.

15 CA-1996-15: Vulnerability in Solaris 2.5 KCMS programs

Original issue date: July 31, 1996
Last revised: October 20, 1997
Vendor information for Sun has been added to the UPDATES section.

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

The text of this advisory was originally released on July 26, 1996, as AUSCERT Advisory AL-96.02, developed by the Australian Computer Emergency Response Team. Because of the seriousness of the problem, we are reprinting the AUSCERT advisory here with their permission. Only the contact information at the end has changed: AUSCERT contact information has been replaced with CERT/CC contact information.

Note that this vulnerability also affects Solaris 2.5.1.

The CERT/CC has received reports that this vulnerability has been exploited.

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

AUSCERT have received a report of a vulnerability in the Sun Microsystems Solaris 2.5 distribution involving the programs kcms_calibrate and kcms_configure. These programs are part of the Kodak Color Management System (KCMS) packages.

This vulnerability may allow any local user to gain root privileges.

Exploit details involving this vulnerability have been made publicly available.

At this stage, AUSCERT is not aware of any official patches. AUSCERT recommends that sites take the actions suggested in Section 3 until official patches are available.

Depending on the local sites' requirements, the Solaris 2.5 KCMS packages may or may not have been installed. AUSCERT recommends that individual sites should determine whether the programs are installed and take appropriate action.

This Alert will be updated as more information becomes available.

1. Description

Solaris 2.5 contains support for the Kodak Color Management System (KCMS), a set of Openwindows compliant API's and libraries to create and manage profiles that can describe and control the colour performance of monitors, scanners, printers and film recorders.

KCMS includes the programs kcms_configure and kcms_calibrate which are used for the configuration and calibration of an X11 window system for use with the KCMS library. When installed, these programs have set-user-id root and set-group-id bin privileges.

A vulnerability involving these programs has been reported. Exploit details involving this vulnerability have been made publicly available.

Depending on the local sites' requirements, the Solaris 2.5 KCMS packages may or may not have been installed.

2. Impact

A local user may be able to create and then write to arbitrary files on the system. This can be leveraged to gain root privileges.

3. Workarounds/Solution

Currently, there are no official patches available. When patches are made available it is suggested the sites install the official

Until official patches are available sites are encouraged to remove the setuid and setgid permissions on the kcms_calibrate and kcms_configure programs. These are typically located in /usr/openwin/bin.

```
# chmod 400 /usr/openwin/bin/kcms_calibrate
# chmod 400 /usr/openwin/bin/kcms_configure
```

Note that this will remove the ability for users to run these programs.

AUSCERT wishes to thanks Marek Krawus of the University of Queensland for his assistance in this matter.

UPDATES

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.

Sun Microsystems, Inc.

Sun Microsystems has provided the following list of patches in response to this advisory:

103879-04 5.5.1
103881-04 5.5.1_x86

103878-04 5.5
103880-04 5.5_x86

Revision History

Oct. 20, 1997 Vendor information for Sun has been added to the UPDATES section

Sep. 24, 1997 Updated copyright statement

Feb. 25, 1997 Introduction - added information that CERT/CC has received reports of this vulnerability being exploited. Added copyright information.

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

Beginning of the AUSCERT text - removed AUSCERT advisory header to avoid confusion.

Aug. 02, 1996 Introduction - added information about Solaris 2.5.1.

16 CA-1996-16: Vulnerability in Solaris admintool

Original issue date: August 5, 1996
Last revised: October 20, 1997
Vendor information for Sun has been added to the UPDATES section.

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

The text of this advisory was originally released on July 30, 1996, as AUSCERT Advisory AL-96.03, developed by the Australian Computer Emergency Response Team. Because of the seriousness of the problem, we are reprinting the AUSCERT advisory here with their permission. Only the contact information at the end has changed: AUSCERT contact information has been replaced with CERT/CC contact information.

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

AUSCERT has received a report of a vulnerability in the Sun Microsystems Solaris 2.x distribution involving the program admintool. This program is used to provide a graphical user interface to numerous system administration tasks.

This vulnerability may allow a local user to gain root privileges.

Exploit details involving this vulnerability have been made publicly available.

At this stage, AUSCERT is not aware of any official patches. AUSCERT recommends that sites take the actions suggested in Section 3 until official patches are available.

1. Description

admintool is a graphical user interface that enables an administrator to perform several system administration tasks on a system. These tasks include the ability to manage users, groups, hosts and other services.

To help prevent different users updating system files simultaneously, admintool uses temporary files as a locking mechanism. The handling of these temporary files is not performed in a secure manner, and hence it may be possible to manipulate admintool into creating or writing to arbitrary files on the system. These files are accessed with the effective uid of the process executing admintool.

In Solaris 2.5, admintool is set-user-id root by default. That is, all file accesses are performed with the effective uid of root. An effect of this is that the vulnerability will allow access to any file on the system. If the vulnerability is exploited to try and create a file that already exists, the contents of that file will be deleted. If the file does not exist, it will be created with root ownership and be world writable.

In earlier versions of Solaris 2.x, admintool is not set-user-id root by default. In this case, admintool runs only with the privileges of the user executing it. However, local users may wait for a specific user to execute admintool, exploiting the vulnerability to create or write files with that specific users' privileges. Again, files created in this manner will be world writable.

2. Impact

A local user may be able to create or write to arbitrary files on the system. This can be leveraged to gain root privileges.

3. Workarounds/Solution

Currently, AUSCERT is not aware of any official patches which address this vulnerability. When official patches are made available, AUSCERT suggests that they be installed.

Until official patches are available sites are encouraged to completely prevent execution of admintool by any user (including root).

```
        # chmod 400 /usr/bin/admintool

        # ls -l /usr/bin/admintool

        -r--------   1 root  sys  303516 Oct 27  1995 /usr/bin/ad-
mintool
```

Note that if only the setuid permissions are removed, it is still possible for users to gain privileges when admintool is executed as root.

AUSCERT recommends that, where possible, admintool should not be used at all until official patches are available. In the interim, system administrators should perform administration tasks by using the command line equivalents. More details on performing these tasks may be found in the Sun documentation set.

AUSCERT wishes to thank Brian Meilak (QUT), Marek Krawus (UQ), Leif Hedstrom, Kim Holburn and Michael James for their assistance in this matter.

UPDATES

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.

Sun Microsystems, Inc.

Sun Microsystems has provided the following list of patches in response to this advisory:

103558-10 5.5.1
103559-07 5.5.1_x86
103247-07 5.5
103245-08 5.5_x86

Revision History

```
Oct. 20, 1997  Vendor information for Sun has been added to the
UPDATES section.

Sep. 24, 1997  Updated copyright statement

Aug. 30, 1996  Removed references to CA-96.16.README.

Beginning of the advisory - removed AUSCERT advisory header
to avoid confusion.
```

17 CA-1996-17: Vulnerability in Solaris vold

Original issue date: August 6, 1996
Last revised: October 20, 1997
Vendor information for Sun has been added to the UPDATES section.

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

The text of this advisory was originally released on August 2, 1996, as AUSCERT Advisory AL-96.04, developed by the Australian Computer Emergency Response Team. We are reprinting the AUSCERT advisory here with their permission. Only the contact information at the end has changed: AUSCERT contact information has been replaced with CERT/CC contact information.

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

AUSCERT has received a report of a vulnerability in the Sun Microsystems Solaris 2.x distribution involving the Volume Management daemon, vold(1M). This program is used to help manage CDROM and floppy devices.

This vulnerability may allow a local user to gain root privileges.

Exploit details involving this vulnerability have been made publicly available.

At this stage, AUSCERT is not aware of any official patches. AUSCERT recommends that sites take the actions suggested in Section 3 until official patches are available.

1. Description

The Volume Management daemon, vold(1M), manages the CDROM and floppy devices. For example, it provides the ability to automatically detect, and then mount, removable media such as CDROMs and floppy devices.

vold is part of the Solaris 2.x Volume Management package (SUNWvolu). It is executed as a background daemon on system startup and runs as root.

When vold detects that a CDROM or floppy has been inserted into a drive, it is configured to automatically mount the media, making it available to users. Part of this process includes the creation of temporary files, which are used to allow the Openwindows File Manager, filemgr(1), to determine that new media has been mounted. These files are created by the action_filemgr.so shared object which is called indirectly by vold through rmmount(1M). The handling of these files is not performed in a secure manner. As vold is configured to access these temporary files with root privileges, it may be possible to manipulate vold into creating or over-writing arbitrary files on the system.

This vulnerability requires that vold be running and media managed by vold, such as a CDROM or floppy, be physically loaded into a drive. Note that a local user need not have physical access to the media drive to exploit this vulnerability. It is enough to wait until somebody else loads the drive, exploiting the vulnerability at that time.

This vulnerability is known to be present in Solaris 2.4 and Solaris 2.5. Solaris distributions prior to Solaris 2.4 are also expected to be vulnerable.

2. Impact

Local users may be able to create or over-write arbitrary files on the system. This can be leveraged to gain root privileges.

3. Workaround

AUSCERT believes the workarounds given in Sections 3.1 or 3.2 will address this vulnerability. Vendor patches may also address this vulnerability in the future (Section 3.3).

3.1 Edit /etc/rmmount.conf

The temporary files which are susceptible to attack are created by the /usr/lib/rmmount/action_filemgr.so.1 shared object which is called indirectly by vold through rmmount(1M). rmmount(1M) can be configured so that it does not create the temporary files, thereby removing this vulnerability.

To our knowledge, configuring rmmount(1M) in this fashion will not affect the functionality of vold. It will, however, remove the ability of the Openwindows File Manager, filemgr(1), to automatically detect newly mounted media.

To prevent rmmount(1M) creating temporary files, sites must edit the /etc/rmmount.conf file and comment out (or remove) any entry which references action_filemgr.so.

The standard /etc/rmmount.conf contains the following entries which must be commented out (or deleted) to remove this vulnerability:

action cdrom action_filemgr.so
action floppy action_filemgr.so

After applying this workaround, an example of /etc/rmmount.conf may look like:

```
# @(#)rmmount.conf 1.2     92/09/23 SMI

#

# Removable Media Mounter configuration file.

#

# File system identification
```

```
ident hsfs ident_hsfs.so cdrom

ident ufs ident_ufs.so cdrom floppy pcmem

ident pcfs ident_pcfs.so floppy pcmem

# Actions

#

# Following two lines commented out to remove vold vulnerability

#

# action cdrom action_filemgr.so

# action floppy action_filemgr.so
```

Note that vold does not have to be restarted for these changes to take effect.

3.2 Remove the Volume Management system

Sites who do not require the vold functionality should remove the complete set of Volume Management packages. These are SUNWvolg, SUNWvolu and SUNWvolr. These packages can be removed using pkgrm(1M).

3.3 Install vendor patches

Currently, AUSCERT is not aware of any official patches which address this vulnerability. When official patches are made available, AUSCERT suggests that they be installed.

AUSCERT wishes to thanks to Leif Hedstrom, Mark McPherson(QTAC), Marek Krawus(UQ), DFN-CERT and CERT/CC for their assistance in this matter.

UPDATES

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.

Sun Microsystems, Inc.

Sun Microsystems has provided the following list of patches in response to this advisory:

104010-01 5.5.1
104011-01 5.5.1_x86
104015-01 5.5
104016-01 5.5_x86

101907-14 5.4
101908-14 5.4_x86

Revision History

Oct. 20, 1997 Vendor information for Sun has been added to the UPDATES section.

Sep. 24, 1997 Updated copyright statement

Aug. 30, 1996 Removed references to CA-96.17.README.

Beginning of the advisory - removed AUSCERT advisory header to avoid confusion.

18 CA-1996-18: Vulnerability in fm_fls

Original issue date: August 14, 1996
Last revised: September 24, 1997
Updated copyright statement

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

The CERT Coordination Center has received reports of a configuration problem in the floating license server for Adobe FrameMaker (fm_fls) that enables non-privileged users to make any file world-readable and world-writable. Exploitation scripts are publicly available.

Any system that includes a setuid version of fm_fls is vulnerable. Adobe Systems reports that the following Adobe products use fm_fls:

Frame Products, version 4
FrameMaker
FrameViewer
FrameBuilder

Frame Products, version 5
FrameMaker
FrameMaker+SGML

The CERT/CC team recommends installing a patch from your vendor. Until you can obtain a patch, we urge you to remove the setuid bit from all instances of fm_fls.

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

I. Description

FrameMaker is a commercial text-processing software package available from Adobe Systems, Inc. It is also available from other vendors as part of their product line offering.

When FrameMaker versions 4.X or 5.X are installed, the installation script provided with FrameMaker installs a file named fm_fls that is setuid to installing user, typically the root user. fm_fls is typically found in the FrameMaker installation tree. Consult your documentation for precise location of fm_fls.

When fm_fls runs, it opens up a log file, which by default is /tmp/fm_fls.log. In normal operation, fm_fls writes logging information about license usage to the named log file. However, when given invalid arguments, fm_fls writes these arguments to the log file, changes the owner of the log file to root or whoever installed fm_fls, changes the permissions to world-readable and world-writable, and then exits. Therefore, by giving fm_fls invalid arguments and naming another file as the log file, a user can make that file world-readable and world-writable.

Adobe Systems reports that fm_fls is installed as setuid root because it registers the license manager program with the the program number mapper, also known as portmap or rpcbind. On some platforms, only the original user (in this case root) or the root user has permission to remove a registration. fm_fls will attempt to remove a previous registration when it is restarted. With fm_fls setuid root, restarting fm_fls ensures that all changes made in the program number mapper are successful because they are done by the same user.

The floating license servers shipped with and installed by FrameMaker 4.X and 5.X are vulnerable. Similarly, any other system that includes a setuid version of fm_fls is vulnerable. Exploitation scripts are publicly available.

II. Impact

Anyone with access to an account on an unpatched system can create world-writable and world-readable files; this can lead to gaining root access.

III. Solution

A. Obtain and install a vendor patch when it becomes available.

In the meantime, remove the setuid bit from all instances of fm_fls. To determine if a system is vulnerable and to disable the programs that are believed to be vulnerable, use the find command we provide below or a variant. Consult your local system documentation to determine how to tailor the find program on your system.

You will need to run the find command on each system you maintain because the command examines files on the local disk only. Substitute the names of your local file systems for FILE_SYSTEM_NAMES in the example. Example local file system names are /, /usr, and /var.

To find all instances of fm_fls and then to remove the setuid bit from them, do the following as root. Note that this is one long command, though we have separated it onto two lines using a back-slash.

```
find FILE_SYSTEM_NAMES -xdev -type f -name fm_fls -perm -04000 \
-print -ok chmod u-s '{}' \;
```

This command will find all files on a system that are

- only in the file system you name (FILE_SYSTEM_NAMES -xdev)
- regular files (-type f)
- named fm_fls
- setuid (-perm -04000)

Once found, those files will

- have their names printed (-print)

- have the setuid mode removed, but only if you type `y' in response to the prompt (-ok chmod u-s '{}' \;)

With the setuid root bit removed, fm_fls must then be started each time by the same user. That user should be root so that the previous registration can be successfully removed no matter what platform fm_fls is running on.

In addition, the log file, license.log, should be stored in a non-public directory; specify this new location with the -log command line argument. Consult the documentation that comes with FrameMaker versions 4.X and 5.X to learn how to do this on your system.

B. Another possible solution is to create a new userid and group, say UID

frame and GID frame, with no one in group frame except for UID frame, and make fm_fls mode 4110. For example, on Solaris 2.4, 2.5, or 2.5.1:

```
- - ---s--x---  1 frame  frame  145736 Aug 24  1995 /usr/lo-
cal/frame5.0/bin/sunxm.s5.sparc/fm_fls
```

this case the log file has to be created manually just once by root (if you keep it permanently in /var/log instead of /tmp) and chown'd/chgrp'd to frame/frame with mode 644 (though fm_fls resets that to 666).

At boot time root runs the frame5.0/bin/fm_fls wrapper which ends up invoking the setuid-frame fm_fls binary. That could be done instead using 'su - frame -c frame_startup_command...' as an extra precaution if UID frame has a real shell. In that case you might as well remove the setuid bit too.

This has been working for about a year.

Appendix A

The following is vendor-supplied information. For the most up-to-date information, contact your vendor.

BSDI

Does not ship Frame with BSD/OS.

Digital Equipment Corporation

Does not distribute this product with its operating systems.

Open Software Foundation (OSF)

Does not support the software with this problem.

Sun Microsystems, Inc.

Does not ship FrameMaker.

The CERT Coordination Center staff thanks Adobe Systems for their support in the development of this advisory.

Revision History

Sep. 24, 1997 Updated copyright statement

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

Aug. 21, 1996 Added Section III.B (provides another possible solution).

Aug. 15, 1996 Added Appendix A - vendor information.

19 CA-1996-19: Vulnerability in expreserve

Original issue date: August 15, 1996
Last revised: September 24, 1997
Updated copyright statement

A complete revision history is at the end of this file. **This advisory supersedes CA-93.09 and CA-93.09a.**

The CERT Coordination Center has received reports of a vulnerability in expreserve. Though this is not a new vulnerability, it is one that is widely known and that many users have not yet patched. The CERT/CC team recommends that you patch your system as soon as possible, as exploitation scripts are publicly available. Appendix A contains the information we have received from vendors. Until you can install a patch, you should apply the workaround 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

Expreserve is a utility that preserves the state of a file being edited by *vi(1)* or *ex(1)* when an edit session terminates abnormally or when the system crashes. Expreserve has a vulnerability that allows users to overwrite any file on the system. Exploitation scripts are publicly

II. Impact

By exploiting this vulnerability, users with access to an account on the system can readily gain root privileges.

III. Solution

A. Apply a patch or workaround provided by your vendor.

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

Berkeley Software Design, Inc.
Cray Research
Data General Corporation
Digital Equipment Corporation
Hewlett-Packard Company
IBM Corporation
NeXT Software, Inc.
Open Software Foundation

The Santa Cruz Operation, Inc.
Sun Microsystems, Inc.

B. Until you are able to apply a patch or workaround, we recommend that you remove the execute permissions on the existing /usr/lib/expreserve program.

Do this as root:

% /usr/bin/chmod a-x /usr/lib/expreserve

This workaround disables expreserve functionality. The result of this workaround is that if *vi(1)* or *ex(1)* is running, and the sessions are interrupted, the files being edited will not be preserved and all edits not explicitly saved by the users will be lost. Encourage users to save their files often.

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.

Berkeley Software Design, Inc.

BSD/OS is not vulnerable to this problem. We ship the current Keith Bostic nvi which does not use the old expreserve scheme to save files (it uses the 4.4BSD-style 1777 tmp directories to store user tmp files in /var/tmp owned by the user and therefore doesn't require a setuid scheme to recover them).

Cray Research

We have fixed this problem at Cray Research in Unicos version 7.0.

Data General Corporation

The binary /usr/lib/expreserve is not a setuid program on DG/UX, any flavor. We are not, therefore, vulnerable to the exploitation described. Nevertheless, the suggested change has been made and will be included in subsequent releases of DG/UX.

Digital Equipment Corporation

This reported problem is not present for Digital's ULTRIX or Digital UNIX Operating Systems Software.

SOURCE:

Digital Equipment Corporation
Software Security Response Team

8/13/96 - DIGITAL EQUIPMENT CORPORATION

Hewlett-Packard Company

```
PROBLEM:  **REVISED 01**  Vulnerability in /usr/lib/expreserve in
HP-UX 9.X and 10.X

PLATFORM: HP 9000 series 300/400s and 700/800s

DAMAGE:   The default permissions of file expreserve(1) are in er-
ror, thereby allowing users to potentially gain root privileges on
the host.

SOLUTION: Apply patch PHCO_6363 (series 700/800, HP-UX 9.x), or

                        PHCO_7833 (series 300/400, HP-UX 9.x), or

                        PHCO_8652 (series 700/800, HP-UX 10.0X), or

                        PHCO_8653 (series 700/800, HP-UX 10.10), or

                        PHCO_8654 (series 700/800, HP-UX 10.20).

Perform the actions described below in releases of HP-UX prior to
9.X.)

AVAILABILITY:  All patches are available now.

CHANGE SUMMARY:  New patches available for releases of HP-UX 10.XX.
```

A. Additional patches for HP-UX have been released to address the vulnerability originally appearing in the 18 July 1996 version of the Hewlett-Packard bulletin.

A private communication to HP described a vulnerability that allows ordinary users to potentially gain super-user privileges. The default permission for the file /usr/lib/expreserve (or on HP-UX 10.X /usr/lbin/expreserve) needs only minimal privileges. If the patches mentioned above are applied the vulnerability cannot be exploited.

In case no patches is available for your host HP-UX release, system administrators are asked to perform the following action to achieve the same result.

Fixing the problem

They should:

$ su root
# chmod 0555 /usr/lib/expreserve

For HP-UX 10.X systems applying the patches specified above is now in order.

Hewlett-Packard recommends that all customers concerned with the security of their HP-UX systems either apply the appropriate patch or perform the actions described above as soon as possible.

How to Install the Patch

1. Determine which patch is appropriate for your hardware platform and operating system:

PHCO_6363 (series 700/800, HP-UX 9.x)
PHCO_7833 (series 300/400, HP-UX 9.x)
PHCO_8652 (series 700/800, HP-UX 10.0X)
PHCO_8653 (series 700/800, HP-UX 10.10)
PHCO_8654 (series 700/800, HP-UX 10.20)

2. 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 HP-UX patch downloading process via email and other services available.

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

3. Apply the patch to your HP-UX system.

4. Examine /tmp/update.log (in 9.X) or /var/adm/sw/swinstall.log (in 10.X), for any relevant WARNINGs or ERRORs.

Impact:
These patches for HP-UX releases 9.X and 10.X provide a proper permissions /usr/lib/expreserve which fixes the vulnerability. No patches will be available for versions of HP-UX older than 9.X. Instead, the workaround is described above.

IBM Corporation

AIX versions 3.2.5, 4.1, and 4.2 are not vulnerable to this particular problem.

IBM and AIX are registered trademarks of International Business Machines Corporation.

NeXT Software, Inc.

This problem was fixed in or before release 3.3 of NeXTstep.

Open Software Foundation

OSF's OSF/1 R1.3 is not effected by this vulnerability.

The Santa Cruz Operation, Inc.

SCO Operating Systems are not vulnerable to this problem.

Silicon Graphics, Inc.

The Silicon Graphics implementation of expreserv is setgid sys and not setuid root as reported in the CERT* advisory. As such this redefines the exposure to a setgid sys issue. Exploit would have to occur on group sys writable files, however, on a default configured IRIX system there are no system critical files that are group sys writable and therefore exposure and exploit does not exist.

Silicon Graphics will not be releasing a patch for this issue, however, the issue will be corrected in future releases of IRIX.

If desired, the setgid permission of the expreserv could be removed however, this will disable the recovery functions of the *vi(1)* and *ex(1)* editors. This functionality could be fixed by manually creating directories for each user in /var/preserve directory.

Sun Microsystems, Inc.

System	Patch ID	Filename	MD5 Checksum
SunOS 4.1.1	101080-01	101080-01.tar.Z	53c8a5c4eee770924560c5fc100542a3
SunOS 4.1.2	101080-01	101080-01.tar.Z	53c8a5c4eee770924560c5fc100542a3
SunOS 4.1.3	101080-01	101080-01.tar.Z	53c8a5c4eee770924560c5fc100542a3
SunOS 4.1.3C	101080-01	101080-01.tar.Z	53c8a5c4eee770924560c5fc100542a3
SunOS 4.1.3_U1	101579-01	101579-01.tar.Z	327b89942b02c4cb15bb80bf61b2df94
SunOS 4.1.4	Not vulnerable		
Solaris 2.0	101119-01	101119-01.tar.Z	No longer available
Solaris 2.1	101089-01	101089-01.tar.Z	No longer available
Solaris 2.2	101090-01	101090-01.tar.Z	e9ff98823abbc75d95410a0cb7856644
Solaris 2.3	Vulnerable; no patch made		
Solaris 2.4	102756-01	102756-01.tar.Z	61f4a48ddba41ae1c27e70b84f4c8d87
Solaris 2.4_x86	102757-01	102757-01.tar.Z	1f2b7f3824565ef849eb3c4677567399
Solaris 2.5	Not vulnerable		
Solaris 2.5.1	Not vulnerable		

The CERT Coordination Center thanks all the vendors who provided input for this advisory.

Revision History

Sep. 24, 1997 Updated copyright statement

Dec. 20, 1996 Appendix A, HP - revised information from vendor has been included.

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

Aug. 28, 1996 Appendix A, SGI - added an entry for this vendor.

Aug. 21, 1996 Appendix A, Sun - added more patch information.

20 CA-1996-20: Sendmail Vulnerabilities

Original issue date: September 18, 1996
Last revised: December 9, 1998
Updated vendor information for Silicon Graphics, Inc.

A complete revision history is at the end of this file. **See also CA-96.24.sendmail.daemon.mode.html for information about additional vulnerabilities in sendmail.**

The CERT Coordination Center has received reports of two security problems in sendmail that affect all versions up to and including 8.7.5. By exploiting the first of these vulnerabilities, users who have local accounts can gain access to the default user, which is often daemon. By exploiting the second vulnerability, any local user can gain root access.

The CERT/CC team recommends installing vendor patches or upgrading to the current version of sendmail (8.7.6). Until you can do so, we urge you to apply the workaround provided in Sec. III.C. In all cases, be sure to take the extra precautions listed in Sec. III.D.

For beta testers of sendmail 8.8: The vulnerabilities described in this advisory have been fixed in the beta version.

We will update this advisory as we receive additional information. Please check advisory files regularly for updates that relate to your site. In addition, you can check ftp://ftp.cert.org/pub/latest_sw_versions/sendmail to identify the most current version of sendmail.

I. Description

There are two vulnerabilities in all versions of sendmail up to and including sendmail 8.7.5. The first vulnerability is a resource starvation problem and the second is a buffer overflow problem.

Resource Starvation

When email is forwarded to a program using a .forward file or an :include: statement within a .forward or alias file, that program is executed as the owner of the .forward file or the file referenced by the :include: statement. Similarly, if email is forwarded to a file, that file is opened as the owner of the .forward file or the file referenced by the :include: statement. The file owner is called the "controlling user."

If the message cannot be delivered immediately, the name of the controlling user is written into the queue file along with the other delivery information so that the appropriate permissions can be acquired when the mail queue is processed.

Only the name of the controlling user is written in the queue file. This name is derived by calling the system routine *getpwuid(3)* on the user id of the file owner. If getpwuid fails, the sendmail default user (defined by the DefaultUser option in 8.7 and by the "u" and "g" options in older releases) is assumed.

In some cases, the system can be forced into resource starvation, thus forcing *getpwuid(3)* to fail even though an entry exists in /etc/passwd corresponding to that uid. Since getpwuid has no way of portably returning an error meaning "resource failure" as distinct from "user id not found," sendmail has no way of distinguishing between these cases; it assumes that the uid is unknown and falls back to the default user.

By starving sendmail of specific resources, sendmail will create files owned by the default user. Once created, these files can be used to access other files owned by the default user. In addition, these files owned by the default user can be used to leverage access to other privileged users on the system.

Buffer Overflows

There are several buffer overflows present in sendmail version 8.7.5 and earlier. Some of the buffer overflows could result in local users gaining unauthorized root access.

Significant work has been done on sendmail version 8.8 (now in beta test) to eliminate the problem, and the code changes originally planned for 8.8 have been backported to 8.7.6 to address these vulnerabilities.

II. Impact

Resource Starvation

Anyone with access to an account on the system can run programs or write files as the default user. The danger of compromising the default user depends primarily on the other files in your system owned by that user.

For example, on many systems the line printer spool directory (e.g., /var/spool/lpd) is owned by daemon; because the line printer subsystem runs setuid root, it may be possible to gain additional privileges. However, some other systems have no files owned by user daemon on the default system, and the only files owned by group daemon are not writable by that group; hence, the danger is minimal.

Buffer Overflows

Anyone with access to an account on the system can gain root access.

III. Solution

Install a patch from your vendor if one is available (Sec. A) or upgrade to the current version of sendmail (Sec. B). Until you can take one of those actions, we recommend applying the workaround described in Sec. C. This workaround addresses the resource starvation problem but not buffer overflows.

In all cases, you should take the precautions listed in Sec. D.

Note to beta testers of sendmail 8.8: The vulnerabilities described in this advisory have been fixed in the beta version of 8.8.

A. Install a vendor patch.

Below is a list of the vendors who have provided information about sendmail. Details are in Appendix A of this advisory; we will update the appendix as we receive more information. If your vendor's name is not on this list, please contact the vendor directly.

Digital Equipment Corporation
FreeBSD
Hewlett-Packard Company
IBM Corporation
Linux
Open Software Foundation
The Santa Cruz Operation
Silicon Graphics Inc.
Sun Microsystems, Inc.

B. Upgrade to the current version of sendmail.

Install sendmail 8.7.6. This version is a "drop in" replacement for 8.7.x. There is no patch for 8.6.x. If you are using version 8.6 or earlier, you need to upgrade to the current version and rebuild your sendmail.cf files. Upgrading to version 8.7.6 addresses both vulnerabilities described in this advisory.

Sendmail 8.7.6 is available from

ftp://ftp.sendmail.org/ucb/src/sendmail/sendmail.8.7.6.tar.gz

ftp://ftp.cert.org/pub/tools/sendmail/sendmail.8.7.6.tar.gz

ftp://ftp.cert.dfn.de/pub/tools/net/sendmail/sendmail.8.7.6.tar.gz

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

MD5 (sendmail.8.7.6.tar.gz) = 4a1f2179c53c9106bc8d7738f4d55667

Also in that directory are .Z and .sig files. The .Z file contains the same bits as the .gz file, but is compressed using UNIX compress instead of gzip. The .sig is Eric Allman's PGP signature for the uncompressed tar file. The key fingerprint is

```
Type bits/keyID    Date       User ID

  pub  1024/BF7BA421 1995/02/23 Eric P. Allman <eric@CS.Berkeley.EDU>

           Key fingerprint =  C0 28 E6 7B 13 5B 29 02  6F 7E 43 3A 48 4F 45 29

                              Eric P. Allman  <eric@Reference.COM>

                              Eric P. Allman <eric@Usenix.ORG>

                              Eric P. Allman <eric@Sendmail.ORG>

                              Eric P. Allman <eric@CS.Berkeley.EDU>
```

We strongly recommend that when you change to a newXS version of sendmail 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 the sendmail release. Consult the cf/README file for a more complete explanation. Creating your configuration files using this method makes it easier to incorporate future changes to sendmail into your configuration files.

For sites that use the ampersand character ('&') in the gecos field of /etc/passwd, they should be aware that this may cause the full name returned to be corrupted or empty. (See man (4) passwd for further details on the purpose of the ampersand character in the gecos field.) Therefore when configuring sendmail, sites may also wish to ensure that information in the gecos field is explicitly complete, rather than rely on name expansion using the ampersand character.

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 sendmail version 8.7.x. 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.

C. Apply a workaround.

Resource Starvation

Eric Allman, the author of sendmail, has provided the following workaround to the resource starvation vulnerability.

Using smrsh as "prog" mailer limits the programs that can be run as the default user. Smrsh does not limit the files that can be written, but less damage can be done by writing files directly.

The damage can be almost entirely constrained by ensuring that the default user is an innocuous one. Sendmail defaults to 1:1 (daemon) only because that is reasonably portable. A special "mail-null" account that is used only for this purpose would be better. This user should own no files and should have neither a real home directory nor a real shell. A sample password entry might be:

```
mailnull:*:32765:32765:Sendmail Default
User:/no/such/dir:/dev/null
```

A corresponding entry should be made in /etc/group:

```
mailnull:*:32765:
```

These assume that there are no other users or groups with id = 32765 on your system; if there are, pick some other unique value.

NOTE: When allocating a numeric uid to the "mailnull" user you should be careful to ensure that this value is less than the value of the UID_MAX kernel variable, if your system implements this variable. To check whether your system implements this variable (and the value that it uses), check for a reference to it in the "limits.h" header file, which should be located in the directory /usr/include, or one of its subdirectories. For further information on the use and content on the "limits.h" header file, see the man (4) limits.

After creating this user, change the line in /etc/sendmail.cf reading

```
O DefaultUser=1:1
```

to read

```
O DefaultUser=mailnull
```

If you are running 8.6.*, you will have to change the lines reading

```
Ou1

Og1
```

to read

```
Ou32765

Og32765
```

Finally, if you are using the m4(1)-based sendmail configuration scheme provided with sendmail 8.7.*, you should add the following line to the m4 input file, usually named sendmail.mc:

```
define(`confDEF_USER_ID', 32765:32765)
```

The actual values should, of course, match those in the passwd file.

Buffer Overflows

There is no workaround for the buffer overflow problem. To address this problem, you must apply your vendor's patches or upgrade to the current version of sendmail (version 8.7.6).

D. Take additional precautions.

Regardless of which solution you apply, you should take these extra precautions to protect your systems.

- Use the sendmail restricted shell program (smrsh)
- With *all* versions of sendmail, use the sendmail restricted shell program (smrsh). You should do this whether you use vendor-supplied sendmail or install sendmail yourself. Using smrsh gives you improved administrative control over the programs sendmail executes on behalf of users.

  A number of sites have reported some confusion about the need to continue using the sendmail restricted shell program (smrsh) when they install a vendor patch or upgrade to a new version of sendmail. You should always use the smrsh program.

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

  smrsh is also distributed with some operating systems.

- Use mail.local

- If you run /bin/mail based on BSD 4.3 UNIX, replace /bin/mail with mail.local, which is included in the sendmail distribution. It is also included with some other operating systems distributions, such as FreeBSD.

  Although the current version of mail.local is not a perfect solution, it is important to use it because it addresses vulnerabilities that are being exploited. For more details, see CERT advisory CA-95.02.

  Note that as of Solaris 2.5 and beyond, mail.local is included with the standard distribution. To use mail.local, replace all references to /bin/mail with /usr/lib/mail.local. If you are using the M4(1)-based configuration scheme provided with sendmail 8.X, add the following to your configuration file:

  define(`LOCAL_MAILER_PATH', /usr/lib/mail.local)

- WARNING: Check for executable copies of old versions of mail programs

- If you leave executable copies of older versions of sendmail installed in /usr/lib (on some systems, it may be installed elsewhere), the vulnerabilities in those versions could be exploited if

an intruder gains access to your system. This applies to sendmail.mx as well as other sendmail programs. Either delete these versions or change the protections on them to be non-executable.

Similarly, if you replace /bin/mail with mail.local, remember to remove old copies of /bin/mail or make them non-executable.

Appendix A: Vendor Information

Below is a list of the vendors who have provided information for this advisory. We will update this appendix as we receive additional information. If you do not see your vendor's name, please contact the vendor directly.

Berkeley Software Design, Inc.

BSDI has released a patch for BSD/OS V2.1 to update sendmail to the 8.7.6 version. The patch is available from the patches@BSDI.COM mailback server
or via ftp at: ftp://ftp.BSDI.COM/bsdi/patches/patches-2.1/U210-024

Digital Equipment Corporation

[About the resource starvation problem]

Source:

Software Security Response Team

08.SEP.1996

At the time of writing this document, patches (binary kits) for Digital's UNIX related operating systems are being developed. Digital will provide notice of availability for remedial kits through AES services (DIA, DSNlink FLASH), placed in the public FTP patch service domain and also be available from your normal Digital Support channel.

```
ftp://ftp.service.digital.com/public/{OS}/{vn.n}
                                              |     |
                                              |     |--version
                                              |--osf or ultrix
```

- DIGITAL EQUIPMENT CORPORATION
9/96

FreeBSD

All currently released FreeBSD distributions have this vulnerability, as we distribute sendmail 8.7.x as part of our operating system. However, our -current and -stable source distributions were

updated on 18 Sep 1996 to sendmail 8.7.6. Users tracking -current or -stable are advised to upgrade and recompile sendmail at their earliest convinience.

An official FreeBSD security advisory, including patches to close this vulnerability in FreeBSD 2.1.5 will be available shortly. The security advisory will appear at ftp://freebsd.org/pub/CERT/patches/SA-96:18/ when available.

Hewlett-Packard Company

HPSBUX9704-059

HEWLETT-PACKARD SECURITY BULLETIN: #00059, 30 April 1997

Description: Sendmail patches for HP-UX releases 9.X thru 10.20

Security Bulletins are available from the HP Electronic Support Center via electronic mail.

User your browser to get to the HP Electronic Support Center page at:
http://us-support.external.hp.com (for US, Canada, Asia-Pacific, & Latin-America) and
http://europe-support.external.hp.com (for Europe).

IBM Corporation

The following APARs are being developed and will be available shortly. See the appropriate release below to determine your action.

AIX 3.2

Apply the following fixes to your system:

APAR - IX61303 IX61307

AIX 4.1

Apply the following fixes to your system: APAR - IX61162 IX61306

To determine if you have this APAR on your system, run the following command:

instfix -ik IX61162 IX61306

AIX 4.2

Apply the following fixes to your system: APAR - IX61304 IX61305

To determine if you have this APAR on your system, run the following command:

instfix -ik IX61304 IX61305

To Order

APARs may be ordered using Electronic Fix Distribution (via FixDist) or from the IBM Support Center. For more information on FixDist, http://service.software.ibm.com/aixsupport/ or send e-mail to aixserv@austin.ibm.com with a subject of "FixDist".

IBM and AIX are registered trademarks of International Business Machines Corporation.

Linux

[For the resource starvation problem:]

Debian Linux: not vulnerable (uses smail)

Red Hat and derivatives:
ftp://ftp.redhat.com/pub/redhat-3.0.3/i386/updates/RPMS/sendmail*

Open Software Foundation

OSF's OSF/1 R1.3.2 is not vulnerable to these types of attacks described in the resource starvation sections of the advisory.

OSF's OSF/1 R1.3.2 is vulnerable to the buffer overflow problems. We will address the problem in our next maintenance release.

The Santa Cruz Operation

Any SCO operating system running a version of sendmail provided by SCO is vulnerable to this problem. SCO is providing Support Level Supplement (SLS) oss443a for the following releases to address this issue:

SCO Internet FastStart release 1.0.0
SCO OpenServer releases 5.0.0 and 5.0.2

This SLS provides a pre-release version of sendmail release 8.7.6 for these platforms. SCO hopes to have a final version of sendmail 8.7.6 available to address both issues mentioned in this advisory in the near future.

Note that only SCO Internet FastStart uses sendmail as the default mail system. All other SCO operating systems use other mail systems such as the Multi-Channel Memorandum Distribution Facility (MMDF) or the "mailsurr" mail system as the default, and as such are not vulnerable to this problem unless otherwise configured to use sendmail.

SCO intends to provide a similar patch for SCO UnixWare release 2.1.0 in the near future.

When configured to use a version of sendmail provided by SCO, releases prior to the ones mentioned here are also vulnerable, but no plans have yet been made concerning patches for these earlier releases.

You can download SLS oss443a as shown below.

Anonymous ftp (World Wide Web URL) ftp://ftp.sco.COM/SSE/oss443a (SLS image)
ftp://ftp.sco.COM/SSE/oss443a.ltr.sse (cover letter/install notes)

Compuserve

SLS oss443a is also available in the SCO Forum on Compuserve.

SCO Online Support (SOS) BBS

SLS oss443a can also be downloaded interactively via X, Y, or Z MODEM or Kermit, using the SCO Online Support System (SOS). Follow the menu selections under "Toolchest" from the main SOS menu.

The phone numbers available for interactive transfer from SOS are:

1-408-426-9495 (USA)
+44 (0)1923 210 888 (United Kingdom)

Checksums

```
sum -r

   ------

   13804   630 oss443a

   35304    14 oss443a.ltr.sse

   MD5

   ---

   MD5 (oss443a) = 549260a71ca76f4e98dd38bccb72748c

   MD5 (oss443a.ltr.sse) = 7475d83f0db64a1af69eb66cd392a9d3
```

Be sure to keep track of the README file at ftp://ftp.sco.COM/SSE/README for updates to this supplement.

If you have further questions, contact your support provider. If you need to contact SCO, please send electronic mail to support@sco.COM , or contact SCO as follows:

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

1-800-347-4381 (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-5:30pm Greenwich Mean Time (GMT)

+44 (0)1923 816344 (voice)
+44 (0)1923 817781 (fax) XS

Silicon Graphics, Inc.

Please refer to Silicon Graphics Inc. Security Advisory, "IRIX mail(1)/rmail(1M)/sendmail(1M) Security Vulnerabilities," Number: 19980604-02-PX, distributed September 29, 1998 for additional information relating to this vulnerability.

The primary SGI anonymous FTP site for security information and patches is sgigate.sgi.com (204.94.209.1). Security information and patches are located under the directories ~ftp/security and ~ftp/patches, respectively. The Silicon Graphics Security Headquarters Web page is accessible at the URL http://www.sgi.com/Support/security/security.html.

Sun Microsystems, Inc.

Sun Microsystems has provided the following list of patches in response to this advisory:

103594-10 5.5.1
103595-10 5.5.1_86
102980-13 5.5
102981-13 5.5_x86
102066-18 5.4
102064-17 5.4_x86
101739-17 5.3
102423-07 4.1.4
101665-10 4.1.3_U1

The CERT Coordination Center staff thanks Eric Allman, the author of sendmail, for his extensive assistance with this advisory, Wolfgang Ley of DFN-CERT and members of the AUSCERT for their contributions, and D. J. Bernstein of the University of Illinois at Chicago for reporting the resource starvation vulnerability.

Revision History

```
Dec.  9, 1998  Updated vendor information for Silicon Graphics, Inc.

Aug. 24, 1998  Updated vendor information for Silicon Graphics, Inc.

Oct. 20, 1997  Appendix A - updated vendor information for Sun.

Sep. 24, 1997  Updated copyright statement
```

May 8, 1997 Appendix A - updated vendor information for Hewlett-Packard.

Nov. 21, 1996 Introduction - Added a pointer to CA-96.24 for information on more sendmail vulnerabilities.

Nov. 19, 1996 Appendix A - Updated Hewlett-Packard information to address both problems.

Sep. 21, 1996 Sec. III.B - added instructions on configuring sendmail at sites that use '&' in the gecos filed of /etc/passwd.

Sec. III.C - added a note on uid for "mailnull" user.

Sep. 19, 1996 Sec. III.B - added URL in Australia for sendmail

Acknowledgements - included reference that had been omitted earlier.

Appendix, FreeBSD - added an entry.

Sep. 18, 1996 Appendix, BSDI - added an entry containing patch information.

21 CA-1996-21: TCP SYN Flooding and IP Spoofing Attacks

Original issue date: September 19, 1996
Last revised: November 29, 2000
Updated vendor information for the Linux kernel.

A complete revision history is at the end of this file. **This advisory supersedes the IP spoofing portion of CA-95.01.**

Two "underground magazines" have recently published code to conduct denial-of-service attacks by creating TCP "half-open" connections. This code is actively being used to attack sites connected to the Internet. There is, as yet, no complete solution for this problem, but there are steps that can be taken to lessen its impact. Although discovering the origin of the attack is difficult, it is possible to do; we have received reports of attack origins being identified.

Any system connected to the Internet and providing TCP-based network services (such as a Web server, FTP server, or mail server) is potentially subject to this attack. Note that in addition to attacks launched at specific hosts, these attacks could also be launched against your routers or other network server systems if these hosts enable (or turn on) other TCP services (e.g., echo). The consequences of the attack may vary depending on the system; however, the attack itself is fundamental to the TCP protocol used by all systems.

If you are an Internet service provider, please pay particular attention to Section III and Appendix A, which describes step we urge you to take to lessen the effects of these attacks. If you are the customer of an Internet service provider, please encourage your provider to take these steps.

This advisory provides a brief outline of the problem and a partial solution. We will update this advisory as we receive new information. If the change in information warrants, we may post an updated advisory on comp.security.announce and redistribute an update to our cert-advisory mailing list. As always, the latest information is available at the URLs listed at the end of this advisory.

I. Description

When a system (called the client) attempts to establish a TCP connection to a system providing a service (the server), the client and server exchange a set sequence of messages. This connection technique applies to all TCP connections--telnet, Web, email, etc.

The client system begins by sending a SYN message to the server. The server then acknowledges the SYN message by sending SYN-ACK message to the client. The client then finishes establishing the connection by responding with an ACK message. The connection between the client and

the server is then open, and the service-specific data can be exchanged between the client and the server. Here is a view of this message flow:

```
Client                    Server

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

SYN-------------------->

     <--------------------SYN-ACK

ACK-------------------->

       Client and server can now

       send service-specific data
```

The potential for abuse arises at the point where the server system has sent an acknowledgment (SYN-ACK) back to client but has not yet received the ACK message. This is what we mean by half-open connection. The server has built in its system memory a data structure describing all pending connections. This data structure is of finite size, and it can be made to overflow by intentionally creating too many partially-open connections.

Creating half-open connections is easily accomplished with IP spoofing. The attacking system sends SYN messages to the victim server system; these appear to be legitimate but in fact reference a client system that is unable to respond to the SYN-ACK messages. This means that the final ACK message will never be sent to the victim server system.

The half-open connections data structure on the victim server system will eventually fill; then the system will be unable to accept any new incoming connections until the table is emptied out. Normally there is a timeout associated with a pending connection, so the half-open connections will eventually expire and the victim server system will recover. However, the attacking system can simply continue sending IP-spoofed packets requesting new connections faster than the victim system can expire the pending connections.

In most cases, the victim of such an attack will have difficulty in accepting any new incoming network connection. In these cases, the attack does not affect existing incoming connections nor the ability to originate outgoing network connections.

However, in some cases, the system may exhaust memory, crash, or be rendered otherwise inoperative.

The location of the attacking system is obscured because the source addresses in the SYN packets are often implausible. When the packet arrives at the victim server system, there is no way to determine its true source. Since the network forwards packets based on destination address, the only way to validate the source of a packet is to use input source filtering (see Appendix A).

II. Impact

Systems providing TCP-based services to the Internet community may be unable to provide those services while under attack and for some time after the attack ceases. The service itself is not harmed by the attack; usually only the ability to provide the service is impaired. In some cases, the system may exhaust memory, crash, or be rendered otherwise inoperative.

III. Solution

There is, as yet, no generally accepted solution to this problem with the current IP protocol technology. However, proper router configuration can reduce the likelihood that your site will be the source of one of these attacks.

Appendix A contains details about how to filter packets to reduce the number of IP-spoofed packets entering and exiting your network. It also contains a list of vendors that have reported support for this type of filtering.

NOTE to Internet Service Providers:

We STRONGLY urge you to install these filters in your routers to protect your customers against this type of an attack. Although these filters do not directly protect your customers from attack, the filters do prevent attacks from originating at the sites of any of your customers. We are aware of the ramifications of these filters on some current Mobile IP schemes and are seeking a position statement from the appropriate organizations.

NOTE to customers of Internet service providers:

We STRONGLY recommend that you contact your service provider to verify that the necessary filters are in place to protect your network.

Many networking experts are working together to devise improvements to existing IP implementations to "harden" kernels to this type of attack. When these improvements become available, we suggest that you install them on all your systems as soon as possible. This advisory will be updated to reflect changes made by the vendor

IV. Detecting an Attack

Users of the attacked server system may notice nothing unusual since the IP-spoofed connection requests may not load the system noticeably. The system is still able to establish outgoing connections. The problem will most likely be noticed by client systems attempting to access one of the services on the victim system.

To verify that this attack is occurring, check the state of the server system's network traffic. For example, on SunOS this may be done by the command:

```
netstat -a -f inet
```

Note that use of the above command depends on the OS version, for example for a FreeBSD system use

```
netstat -s |grep "listenqueue overflows"
```

Too many connections in the state "SYN_RECEIVED" could indicate that the system is being attacked.

Appendix A: Reducing IP Spoofed Packets

1. Filtering Information

With the current IP protocol technology, it is impossible to eliminate IP-spoofed packets. However, you can take steps to reduce the number of IP-spoofed packets entering and exiting your network.

Currently, the best method 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 to prevent a source IP spoofing attack from originating from your site.

The combination of these two filters would prevent outside attackers from sending you packets pretending to be from your internal network. It would also prevent packets originating within your network from pretending to be from outside your network. These filters will *not* stop all TCP SYN attacks, since outside attackers can spoof packets from *any* outside network, and internal attackers can still send attacks spoofing internal addresses.

We STRONGLY urge Internet service providers to install these filters in your routers.

In addition, we STRONGLY recommend customers of Internet service providers to contact your service provider to verify that the necessary filters are in place to protect your network.

2. Vendor Information

The following vendor(s) have reported support for the type of filtering we recommend and provided pointers to additional information that describes how to configure your router. If we hear from other vendors, we will add their information to the "Updates" section at the end of this advisory.

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

Cisco

Refer to the section entitled "ISP Security Advisory" on http://www.cisco.com for an up-to-date explanation of how to address TCP SYN flooding on a Cisco router.

NOTE to vendors:

If you are a router vendor who has information on router capabilities and configuration examples and you are not represented in this list, please contact the CERT Coordination Center at the addresses given in the Contact Information section below. We will update the advisory after we hear from you.

3. Alternative for routers that do not support filtering on the inbound side

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 follow.

On the input to your external interface, that is coming from the Internet to your network, you should block packets with the following addresses:

- Broadcast Networks: The addresses to block here are network 0 (the all zeros broadcast address) and network 255.255.255.255 (the all ones broadcast network).
- Your local network(s): These are your network addresses
- Reserved private network numbers: The following networks are defined as reserved private networks, and no traffic should ever be received from or transmitted to these networks through a router:

```
10.0.0.0     - 10.255.255.255    10/8           (reserved)
127.0.0.0    - 127.255.255.255   127/8          (loopback)
172.16.0.0   - 172.31.255.255    172.16/12      (reserved)
192.168.0.0 - 192.168.255.255   192.168/16     (reserved)
```

The CERT Coordination Center staff thanks the team members of NASIRC for contributing much of the text for this advisory and thanks the many experts who are devoting time to addressing the problem and who provided input to this advisory.

UPDATES

3COM

Please refer to the "Network Security Advisory" for a thorough discussion of how to address TCP SYN flooding attacks on a 3Com router: http://www.3com.com/.

Berkeley Software Design, Inc.

BSDI has patches available.

PATCH

K210-021 (ftp://ftp.bsdi.com/bsdi/patches/patches-2.1/K210-021)

md5 checksum: c386e72f41d0e409d91b493631e364dd K210-021

This patch adds two networking features that can help defeat and detect some types of denial of service attacks.

This patch requires U210-025 which provides new copies of *sysctl(8)* and *netstat(1)* for configuration and monitoring of these new features.

PATCH

K210-022 (ftp://ftp.bsdi.com/bsdi/patches/patches-2.1/K210-22)

md5 checksum: 9ec62b5e9cc424b9b42089504256d926 K210-022

This patch adds a TCP SYN cache which reduces and/or eliminates the effects of SYN-type denial of service attacks such as those discussed in CERT advisory CA 96.21.

PATCH

U210-025 (ftp://ftp.bsdi.com/bsdi/patches/patches-2.1/U210-025)

md5 checksum: d2ee01238ab6040e9b7a1bd2c3bf1016 U210-025

This patch should be installed in conjunction with IP source address check and IP fragmentation queue limit patch (K210-021) and SYN flooding patch (K210-022).

Additional details about these patches are available from

http://www.bsdi.com
ftp://ftp.bsdi.com

Hewlett-Packard Company

HPSBUX9704-060

Description: SYN Flooding Security Vulnerability in HP-UX

HEWLETT-PACKARD SECURITY BULLETIN: #00060

Security Bulletins are available from the HP Electronic Support Center via electronic mail.

User your browser to get to the HP Electronic Support Center page at: http://us-support.external.hp.com (for US, Canada, Asia-Pacific, & Latin-America) or http://europe-support.external.hp.com (for Europe).

IBM Corporation

Any system that is connected to a TCP/IP-based network (Internet or intranet) and offers TCP-based services is vulnerable to the SYN flood attack. The attack does not distinguish between operating systems, software version levels, or hardware platforms; all systems are vulnerable. IBM has released AIX operating system fixes for the SYN flood vulnerability.

NOTE: If you are using the IBM Internet Connection Secured Network Gateway (SNG) firewall software, you must also apply the fixes listed in the next section.

The following Automated Program Analysis Reports (APARs) for IBM AIX are now available to address the SYN flood attack:

AIX 3.2.5

No APAR available; upgrade to AIX 4.x recommended

AIX 4.1.x

APAR - IX62476

AIX 4.2.x

APAR - IX62428

Fixes for IBM SNG Firewall

The following Automated Program Analysis Reports (APARs) for the IBM Internet Connection Secured Network Gateway firewall product are now available to address the SYN flood and "Ping o' Death" attacks:

NOTE: The fixes in this section should ONLY be applied to systems running the IBM Internet Connection Secured Network Gateway (SNG) firewall software. They should be applied IN ADDITION TO the IBM AIX fixes listed in the previous section.

IBM SNG V2.1

APAR - IR33376 PTF UR46673

IBM SNG V2.2

APAR - IR33484 PTF UR46641

Obtaining Fixes

IBM AIX APARs may be ordered using Electronic Fix Distribution (via the FixDist program), or from the IBM Support Center. For more information on FixDist, and to obtain fixes via the Internet, please reference http://service.software.ibm.com/aixsupport/ or send electronic mail to "aixserv@austin.ibm.com " with the word "FixDist" in the "Subject:" line.

Linux

A patch for version 2.0.29 of the linux kernel source is available from:
http://www.kernel.org/pub/linux/kernel/v2.0/patch-2.0.30.gz.

The patch allows tcp/ip processing to continue as normal, until the queue gets close to full. Then, instead of just sending the synack back, it sends a syn cookie back, and waits for a response to IT before sending the synack. When it sends the cookie, it clears the syn from the queue, so while under attack, the queue will never fill up. Cookies expire shortly after they are sent. Basically this prevents people from filling up the queue completely. No one flooding from a spoof will be able to reply to the cookie, so nothing can be overloaded. And if they aren't flooding from a spoof, they would be getting a cookie they would have to respond to, and would have a hard time responding to all the cookies and continuing the flood.

Livingston Enterprises, Inc.

Refer to the following Applications Note for more information on configuring a Livingston IRX or PortMaster to help block outgoing SYN attacks from an ISP's users:
ftp://ftp.livingston.com/pub/le/doc/notes/filters.syn-attack.

Silicon Graphics, Inc.

Updated Silicon Graphics information concerning SYN attacks can be found in SGI Security Advisory, "IRIX IP Spoofing/TCP Sequence Attack Update," 19961202-01-PX, issued on August 6, 1998.

Patches are available via anonymous FTP and your service/support provider.

The SGI anonymous FTP site is sgigate.sgi.com (204.94.209.1) or its mirror, ftp.sgi.com. Security information and patches can be found in the ~ftp/security and ~ftp/patches directories, respectfully.

For subscribing to the wiretap mailing list and other SGI security related information, please refer to the Silicon Graphics Security Headquarters website located at:

http://www.sgi.com/Support/security

Sun Microsystems, Inc.

Sun published a bulletin on October 9, 1996--Sun security bulletin number 00136. Sun Security Bulletins are available via the security-alert@sun.com alias and on SunSolve.

Note: Advisories from vendors listed in this section can also be found at ftp://ftp.cert.org/pub/vendors/

Revision History

Nov. 29, 2000 Updated vendor information for the Linux kernel.

Aug. 24, 1998 Updated vendor information for Silicon Graphics, Inc.

Sep, 24, 1997 Updated copyright statement

July 18, 1997 Updates - added information

May 08, 1997 Updates - updated vendor information for Hewlett-Packard.

Jan. 02, 1997 Updates - added or modified vendor information for SGI, Livingston, HP, 3COM.

Dec. 19, 1996 Updates - corrected Sun Microsystems security-alert email address.

Dec. 10, 1996 Appendix A, #3 - corrected next to last reserved private network number entry.

Dec. 09, 1996 Updates - added IBM patch information.

Nov. 12, 1996 Introduction, paragraph 2 - added some clarification.

Oct. 10, 1996 Updates - added a pointer to Sun Microsystems advisory.

added a pointer to the CERT /pub/vendors directory.

Oct. 08, 1996 Appendix A, #3 - revised the last item, reserved private network numbers

Updates - added BSDI patch information.

Oct. 07, 1996 Updates - added a pointer to Silicon Graphics advisory.

Sep. 24, 1996 Modified the supersession statement.

22 CA-1996-22: Vulnerabilities in bash

Original issue date: October 8, 1996
Last revised: September 24, 1997
Updated copyright statement

A complete revision history is at the end of this file. The original technical content for this advisory was published by the IBM-ERS response team and is used here with their permission.

This advisory describes two problems with the GNU Project's Bourne Again SHell (bash): one in yy_string_get() and one in yy_readline_get().

The vulnerability in yy_string_get() allows the character with value 255 decimal to be used as a command separator. When used in environments where users provide strings to be used as commands or arguments to commands, bash can be tricked into executing arbitrary commands.

When the advisory was first published, was not clear whether the problem with yy_readline_get() resulted in an exploitable vulnerability. As of November 1996, it appears that the problem is not exploitable in yy_readline_get.

The problems affect bash versions 1.14.6 and earlier.

The CERT/CC team recommends that you upgrade to bash 1.14.7 as soon as possible, as discussed in Section III.A below. Section III.B contains a patch for 1.14.7, which we recommend using to address the yy_readline_get() problem.

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. Introduction

The GNU Project's Bourne Again SHell (bash) is a drop-in replacement for the UNIX Bourne shell (/bin/sh). It offers the same syntax as the standard shell, and it also includes additional functionality such as job control, command line editing, and history.

Although bash can be compiled and installed on almost any UNIX platform, its most prevalent use is on "free" versions of UNIX such as Linux, where it has been installed as "/bin/sh" (the default shell for most uses).

The bash source code is freely available from many sites on the Internet.

B. Vulnerability Details

1. Vulnerability in yy_string_get()

There is a variable declaration error in the "yy_string_get()" function in the "parse.y" module of the "bash" source code. This function is responsible for parsing the user-provided command line into separate tokens (commands, special characters, arguments, etc.). The error involves the variable "string", which has been declared to be of type "char *".

The "string" variable is used to traverse the character string containing the command line to be parsed. As characters are retrieved from this pointer, they are stored in a variable of type "int". On systems/compilers where the "char" type defaults to "signed char" this value will be sign-extended when it is assigned to the "int" variable. For character code 255 decimal (-1 in two's complement form), this sign extension results in the value (-1) being assigned to the integer.

However, (-1) is used in other parts of the parser to indicate the end of a command. Thus, the character code 255 decimal (377 octal) will serve as an unintended command separator for commands given to bash via the "-c" option. For example,

```
bash -c 'ls\377who'
```

(where "\377" represents the single character with value 255 decimal) will execute two commands, "ls" and "who".

Note about yy_readline_get()

A similar problem exists with the "yy_readline_get()" function, which is also in the file "parse.y" and which is used to read commands in interactive shells (ones that print a prompt and read from the keyboard, a shell script, or a pipe).

However, it appears that this problem does not produce an exploitable vulnerability.

II. Impact

This unexpected command separator can be dangerous, especially on systems such as Linux where bash has been installed as "/bin/sh," when a program executes a command with a string provided by a user as an argument using the "system()" or "popen()" functions (or by calling "/bin/sh -c string" directly).

This is especially true for the CGI programming interface in World Wide Web servers, many of which do not strip out characters with value 255 decimal. If a user sending data to the server can specify the character code 255 in a string that is passed to a shell, and that shell is bash, the user can execute any arbitrary command with the user-id and permissions of the user running the server (frequently "root").

The bash built-in commands "eval," "source," and "fc" are also potentially vulnerable to this problem.

III. Solution

Install the most current version of bash. On 27 August 1996, Version 1.14.7 of bash was released; It is available from ftp://slc2.ins.cwru.edu/pub/dist/bash-1.14.7.tar.gz.

This version addresses the vulnerability in yy_string_get.

When this advisory was first released, we included a patch for yy_readline_get. It now appears that the patch is unnecessary as the problem is not exploitable in yy_readline_get. Upgrading to the current version of bash is sufficient.

Appendix A

The following is vendor-supplied information. For the most up-to-date information, contact your vendor.

IBM Corporation

AIX does not ship with the bash shell.

IBM and AIX are registered trademarks of International Business Machines Corporation.

Silicon Graphics, Inc.

SGI has distributed bash (version 1.14.6) as part of the Freeware 1.0 CDROM. This collection of software has been compiled for IRIX as a service to our customers, but is furnished without formal SGI support.

The problem identified by IBM in bash is present in the version of bash on the Freeware 1.0 CDROM. This CDROM included both the source code for bash an compiled versions of it.

SGI urges customers to recompile bash after making the changes in parse.y suggested by IBM.

As a service similar to that of the original Freeware 1.0 CDROM, SGI intends to make available a compiled version of bash and its source in the near future. This action does not necessarily imply a commitment to any future support actions for the programs found on the Freeware 1.0 CDROM.

Linux

Patches for the following Linux versions are available.

SuSE 4.2

ftp://ftp.suse.de/suse_update/suse42/a1/bash.tgz

Red Hat 3.0.3

ftp://ftp.redhat.com/pub/redhat/updates/3.0.3/{architecture}/bash-1.14.6.8.{architecture}.rpm

Yggdrasil

Patched bash source and binary tar files are now FTPable from
ftp://ftp.yggdrasil.com/pub/support/fall95 WGS Linux Pro

ftp://ftp.wgs.com/pub/linux/redhat/updates/3.0.3/i386/bash-1.14.6-8.i386.rpm

Caldera

Have built the new bash-1.14.7 code from prep.ai.mit.edu -/pub/gnu. Tested only insofar as to ascertain that the security bug is fixed. Binary and source RPMs live in ftp -

ftp://ftp.caldera.com/pub/cnd-1.0/updates/bash-1.14.7-1.i386.rpm

ftp://ftp.caldera.com/pub/cnd-1.0/updates/bash-1.14.7-1.src.rpm

---

The CERT Coordination Center thanks IBM-ERS for permission to reproduce the technical content in their IBM Emergency Response Service Security Vulnerability Alerts ERS-SVA-E01-1006:004.1 and ERS-SVA-E01-1006:004.2. These alerts are copyrighted 1996 International Business Machines Corporation.

Revision History

```
Sep. 24, 1997  Updated copyright statement

Nov. 13, 1996  Noted that yy_readline_get does not require the patch
included in the original advisory. Removed the patch from Sec. III.

Oct. 14, 1996  Added Appendix A - vendor information.
```

23 CA-1996-23: Vulnerability in Workman

Original issue date: October 28, 1996
Last revised: September 24, 1997
Updated copyright statement

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

The original technical content for this advisory was published by the IBM-ERS response team and is used here with their permission.

There is a vulnerability in the WorkMan compact disc-playing program that affects UNIX System V Release 4.0 and derivatives and Linux systems. When the program is installed set-user-id root, it can be used to make any file on the system world-writable.

To address this problem, you should remove the set-user-id bit from the program.

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

I. Description

WorkMan is a popular program used for playing audio compact disks on local workstation CD-ROM drives that is widely available from many sites around the Internet. Versions of WorkMan are also included with some operating system distributions, such as Linux.

On systems where WorkMan was built and installed using the procedures that are given in "Makefile.linux" or "Makefile.svr4" (in general, this means on Linux systems and UNIX System V Release 4.0 systems), the WorkMan program is installed set-user-id root. This means that when the program is run, it will execute with super-user permissions.

In order to allow signals to be sent to it, WorkMan writes its process-id to a file called /tmp/.wm_pid. The "-p" option to the program allows the user to specify a different file name in which to record this information. When a file is specified with "-p", WorkMan simply attempts to create and/or truncate the file, and if this succeeds, WorkMan changes the permissions on the file so that it is world-readable and world-writable.

In the general case, when WorkMan is installed without the set-user-id bit set, the normal file access permissions provided by the operating system will prevent users from creating or truncating files they are not authorized to create or truncate. However, when WorkMan is installed set-user-id root, this process breaks down (because "root" is allowed to create/truncate any file).

WorkMan does not require the set-user-id bit to work; it is installed this way only on systems that do not make the CD-ROM device file world-readable by default.

Note: The vulnerability described by "r00t" on several mailing lists is not the same one that we describe in this advisory.

II. Impact

A user with access to an account on the system can use the "-p" option to create a file anywhere in the file system or to truncate any file in the file system. The file specified with "-p" will be world-readable and world-writable when WorkMan is finished. This can enable the user to create accounts, destroy log files, and perform other unauthorized actions.

III. Solution

1. Remove the set-user-id bit from the WorkMan program using a command such as

```
chmod u-s /usr/local/bin/workman
```

2. Make the CD-ROM device world-readable using a command such as

```
chmod +r /dev/cdrom
```

On multi-user systems, Step 2 will allow any user to access the contents of the disc installed in the CD-ROM; this may not be desirable in all environments.

The vulnerability described in this advisory is related to the WorkMan program, not to the products of particular vendors. However, if a vendor sends us advice for their users, we will put it in Appendix A.

Appendix A: Vendor Information

This appendix contains advice vendors wish to offer their users. Note that the vulnerability described in this advisory is related to the WorkMan program, not particular vendors' products.

Sun Microsystems, Inc.

Sun does not recommend that workman and other utility programs be installed setuid root (or anything else) unless that step is absolutely necessary. Programs which were not designed with security in mind (and most non-setuid programs are not) are unlikely to have built-in allowances for abuse. The proper way to allow such programs to work is to install them as unprivileged, ordinary software, then modify device permissions as necessary to allow them to function.

When an unprivileged users executes a recent version of the workman program on a properly configured Solaris 2.x system, a message similar to the following appears. (Ellipses added to save space.)

As root, please run

```
chmod 666 /devices/iommu@0,...sd@6,0:c,raw
```

to give yourself permission to access the CD-ROM device.

That's pretty good advice. Of course, if you don't want to give every user access to the contents of a CD (which will sometimes be data or software, and sometimes music) such permissions are not appropriate.

Revision History

```
Sep. 24, 1997  Updated copyright statement
```

24 CA-1996-24: Sendmail Daemon Mode Vulnerability

Original issue date: November 21, 1996
Last revised: September 24, 1997
Updated copyright statement

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

The CERT Coordination Center has received reports of a serious security problem in sendmail that affects versions 8.7 through 8.8.2. By exploiting this vulnerability, any local user can gain root access. Exploitation details involving this vulnerability have been widely distributed.

Independent of this new vulnerability, there are other security problems with older sendmail versions. Even if you are not running a version between 8.7 and 8.8.2, we strongly encourage you to upgrade to the current version of sendmail (8.8.3). See Section IV for details.

The CERT/CC team recommends installing vendor patches or upgrading to the current version of sendmail (8.8.3). Until you can do so, we urge you to apply the workaround provided in Section III.C. In all cases, be sure to take the extra precautions listed in Section III.D.

We will update this advisory as we receive additional information. Please check advisory files regularly for updates that relate to your site. In addition, you can check ftp://ftp.cert.org/pub/latest_sw_versions/sendmail to identify the most current version of sendmail.

I. Description

Sendmail is often run in daemon mode so that it can "listen" for incoming mail connections on the standard SMTP networking port, usually port 25. The root user is the only user allowed to start sendmail this way, and sendmail contains code intended to enforce this restriction.

Unfortunately, due to a coding error, sendmail can be invoked in daemon mode in a way that bypasses the built-in check. When the check is bypassed, any local user is able to start sendmail in daemon mode. In addition, as of version 8.7, sendmail will restart itself when it receives a SIGHUP signal. It does this restarting operation by re-executing itself using the *exec(2)* system call. Re-executing is done as the root user. By manipulating the sendmail environment, the user can then have sendmail execute an arbitrary program with root privileges.

II. Impact

Local users can gain root privileges on the local machine.

III. Solution

Install a patch from your vendor if one is available (Section A) or upgrade to the current version of sendmail (Section B). Until you can take one of those actions, we recommend applying the

workaround described in Section C. In all cases, you should take the precautions described in Section D.

A. Install a vendor patch.

Below is a list of vendors who have provided information about sendmail. Details are in Appendix A of this advisory; we will update the appendix as we receive more information. If your vendor's name is not on this list, please contact the vendor directly.

Berkeley Software Design, Inc. (BSDI)
Data General Corporation
Digital Equipment Corporation
FreeBSD
Hewlett-Packard Company
IBM Corporation
Linux
NeXT Software, Inc.
Open Software Foundation (OSF)
The Santa Cruz Operation, Inc. (SCO)
Silicon Graphics, Inc.
Sun Microsystems, Inc.

B. Upgrade to the current version of sendmail.

Install sendmail 8.8.3. This version is a "drop in" replacement for 8.8.x. There is no patch for any version of sendmail before 8.8.0. If you are running such a version, strongly consider moving to version 8.8.3.

Sendmail 8.8.3 is available from

ftp://ftp.sendmail.org/ucb/src/sendmail/sendmail.8.8.3.tar.gz

ftp://ftp.cert.org/pub/tools/sendmail/sendmail.8.8.3.tar.gz

ftp://ftp.cert.dfn.de/pub/tools/net/sendmail/sendmail.8.8.3.tar.gz

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

MD5 (sendmail.8.8.3.tar.gz) = 0cb58caae93a19ac69ddd40660e01646

Also in that directory are .Z and .sig files. The .Z file contains the same bits as the .gz file, but is compressed using UNIX compress instead of gzip. The .sig is Eric Allman's PGP signature for the uncompressed tar file. The key fingerprint is

```
Type bits/keyID    Date       User ID

  pub  1024/BF7BA421 1995/02/23 Eric P. Allman
<eric@CS.Berkeley.EDU>
```

```
            Key fingerprint =  C0 28 E6 7B 13 5B 29 02  6F 7E 43 3A
48 4F 45 29

                                Eric P. Allman <eric@Reference.COM>

                                Eric P. Allman <eric@Usenix.ORG>

                                Eric P. Allman <eric@Sendmail.ORG>

                                Eric P. Allman
<eric@CS.Berkeley.EDU>
```

When you change to a new version of sendmail, we strongly recommend also changing to the configuration files that are provided with that version. Significant work has been done to make this task easier. (In fact, it is highly likely that older configuration files will not work correctly with sendmail version 8.) It is now possible to build a sendmail configuration file (sendmail.cf) using the configuration files provided with the sendmail release. Consult the cf/README file for a more complete explanation. Creating your configuration files using this method makes it easier to incorporate future changes to sendmail into your configuration files.

Sun sendmail users: A paper is available to help you convert your sendmail configuration files from the Sun version of sendmail to one that works with sendmail version 8.8.x. 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.

C. Apply a workaround.

Eric Allman, the author of sendmail, has provided the following workaround.

This vulnerability relies on a coding error that has existed in sendmail since November 1982, allowing non-root users to start up an SMTP daemon by invoking sendmail as smtpd. However, that error did not have the current negative implications until sendmail added the ability to re-execute when a SIGHUP signal was received; this was added in 8.7.

The anti-smtpd program given in Appendix B refuses to permit sendmail to be invoked as smtpd by a non-root user. It should be installed setuid root in place of sendmail (e.g., as /usr/sbin/sendmail or /usr/lib/sendmail, depending on your system); the real sendmail should be moved to another place. That location should be set in the REAL_SENDMAIL definition, and it should not be accessible by ordinary users. This permits the anti-smtpd program to moderate access to sendmail.

D. Take additional precautions

Regardless of which solution you apply, you should take these extra precautions to protect your systems. These precautions do not address the vulnerabilities described herein, but are recommended as good practices to follow for the safer operation of sendmail.

- Use the sendmail restricted shell program (smrsh)

With *all* versions of sendmail, use the sendmail restricted shell program (smrsh). You should do this whether you use vendor-supplied sendmail or install sendmail yourself. Using smrsh gives you improved administrative control over the programs sendmail executes on behalf of users.

A number of sites have reported some confusion about the need to continue using the sendmail restricted shell program (smrsh) when they install a vendor patch or upgrade to a new version of sendmail. You should always use the smrsh program.

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

smrsh is also distributed with some operating systems.

- Use mail.local

If you run /bin/mail based on BSD 4.3 UNIX, replace /bin/mail with mail.local, which is included in the sendmail distribution. As of Solaris 2.5 and beyond, mail.local is included with the standard distribution. It is also included with some other operating systems distributions, such as FreeBSD.

Although the current version of mail.local is not a perfect solution, it is important to use it because it addresses vulnerabilities that are being exploited. For more details, see CERT advisory CA-95.02.

To use mail.local, replace all references to /bin/mail with /usr/lib/mail.local. If you are using the M4(1)-based configuration scheme provided with sendmail 8.X, add the following to your configuration file:

define(`LOCAL_MAILER_PATH', /usr/lib/mail.local)

- WARNING: Check for setuid executable copies of old versions of mail programs

If you leave setuid executable copies of older versions of sendmail installed in /usr/lib (on some systems, it may be installed elsewhere), the vulnerabilities in those versions could be exploited if an intruder gains access to your system. This applies to sendmail.mx as well as other sendmail programs. Either delete these versions or change the protections on them to be non-executable.

Similarly, if you replace /bin/mail with mail.local, remember to remove old copies of /bin/mail or make them non-executable.

IV. Additional Notes

Two other sendmail vulnerabilities are described in CERT advisory CA-96.20; see that advisory for details.

Since the release of CA-96.20, two additional sendmail vulnerabilities have been discovered and fixed. By upgrading to sendmail version 8.8.3, the two problems, noted below, are also fixed. Note that the wrapper described in Section III.C does not address these vulnerabilities. The best advice is to upgrade to sendmail version 8.8.3.

A. A vulnerability in sendmail Versions 8.8.0 and 8.8.1 has been discovered that allows remote users to execute arbitrary commands with root privileges.

This vulnerability exploits exploiting a problem related to a buffer overflow when converting between 7-bit and 8-bit MIME messages. Versions prior to Version 8.8.0 do not contain this vulnerability. Versions before 8.7.6 contain other unrelated vulnerabilities. This vulnerability is fixed in version 8.8.2 and beyond. The Australian Emergency Response Team (AUSCERT) issued an advisory on this vulnerability, AA-96.06a, available from

http://www.auscert.org.au/

ftp://ftp.auscert.org.au/pub/

B. A problem in sendmail has been reported that permits users on a system to redirect any email in the queue addressed to an unqualified domain name to a host of their choosing

that is, they can steal queued email. In some versions of the resolver, they may also be able to steal queued email addressed to fully qualified addresses. This bug is believed to exist in all versions of sendmail up to and including 8.8.0. It is fixed in version 8.8.1 and beyond.

Appendix A: Vendor Information

Below is a list of the vendors who have provided information for this advisory. We will update this appendix as we receive additional information. If you do not see your vendor's name, please contact the vendor directly.

Berkeley Software Design, Inc. (BSDI)

BSD/OS is vulnerable to the sendmail daemon problem and we have issued an official patch (U210-029) which may be obtained from our mail-back patches server at patches@BSDI.COM or via anonymous ftp from ftp://ftp.bsdi.com/bsdi/patches/patches-2.1/U210-029.

Data General Corporation

The sendmail included with Data General's DG/UX is not subject to this vulnerability.

Digital Equipment Corporation

DIGITAL Engineering is aware of these reported problems and testing is currently underway to determine the impact against all currently supported releases of DIGITAL UNIX and ULTRIX. Patches will be developed (as necessary) and made available via your normal DIGITAL Support channel. Notice will be through normal AES services and DIGITAL'S Web site: http://www.service.digital.com/html/whats-new.html.

FreeBSD

All currently shipping releases of FreeBSD are affected, including the just released 2.1.6. An update for 2.1.6 will be available shortly. This problem has been corrected in the -current sources. In the mean time, FreeBSD users should follow the instructions in the CERT advisory. Sendmail will compile and operate "out of the box" on FreeBSD systems.

Hewlett-Packard Company

HPSBUX9704-059

HEWLETT-PACKARD SECURITY BULLETIN: #00059, 30 April 1997

Description: Sendmail patches for HP-UX releases 9.X thru 10.20

Security Bulletins are available from the HP Electronic
Support Center via electronic mail.

User your browser to get to the HP Electronic Support Center page at:
http://us-support.external.hp.com (for US, Canada, Asia-Pacific, & Latin-America) or
http://europe-support.external.hp.com (for Europe).

IBM Corporation

See the appropriate release below to determine your action.

AIX 3.2

No fix required. AIX 3.2 sendmail is not vulnerable.

AIX 4.1

No fix required. AIX 4.1 sendmail is not vulnerable.

AIX 4.2

AIX 4.2 sendmail is vulnerable.

APAR IX63068 will be available shortly.

To determine if you have this APAR on your system, run the following command:

```
instfix -ik IX63068
```

To Order

APARs may be ordered using Electronic Fix Distribution (via FixDist) or from the IBM Support Center. For more information on FixDist, reference URL:
http://service.software.ibm.com/aixsupport/ or send e-mail to aixserv@austin.ibm.com with a subject of "FixDist".

IBM and AIX are registered trademarks of International Business Machines Corporation.

Linux

Linux has provided these URLs for S.u.S.E. Linux:

ftp://ftp.suse.de/suse_update/S.u.S.E.-4.3/sendmail

ftp://ftp.gwdg.de/pub/linux/suse/suse_update/S.u.S.E.-4.3/sendmail

Checksums for the files in these directories:

```
6279df0597c972bff65623da5898d5dc  sendmail.tgz

0c0d20eecb1019ab4e629b103cac485c  sendmail-8.8.3.dif

0cb58caae93a19ac69ddd40660e01646  sendmail-8.8.3.tar.gz
```

Caldera OpenLinux has released a security advisory, available from

http://www.caldera.com/tech-ref/cnd-1.0/security/SA-96.06.html

Red Hat has patched sendmail 8.7.6.

The fixes are available from

Red Hat Linux/Intel:
rpm -Uvh ftp://ftp.redhat.com/updates/4.0/i386/sendmail-8.7.6-5.i386.rpm

Red Hat Linux/Alpha:
rpm -Uvh ftp://ftp.redhat.com/updates/4.0/axp/sendmail-8.7.6-5.axp.rpm

NeXT Software, Inc.

NeXT is not vulnerable to the problem described in Section IV.A. NeXT is vulnerable to the problem described in Section IV.B, and it will be fixed in release 4.2 of OpenStep/Mach.

Open Software Foundation (OSF)

OSF/1 R1.3 is not vulnerable to this problem.

The Santa Cruz Operation, Inc. (SCO)

SCO is investigating the problem and will have more information in the near future.

If we find that patches are needed, please check the following URLs and this advisory appendix.

ftp://ftp.sco.com/SLS/README

ftp://ftp.sco.com/SSE/README

Silicon Graphics, Inc.

Silicon Graphics has historically provided a version 8.6.x sendmail program. The most recent SGI sendmail patch (1502) provides a version 8.6.12 sendmail program also.

The versions of sendmail provided in the distributed Silicon Graphics IRIX operating system versions 5.2, 5.3, 6.0, 6.0.1, 6.1, 6.2 and 6.3 (and in SGI patch 1502, which is the latest released patch for sendmail) are not vulnerable to the exploitation as described in the CERT Advisory CA-96.24.

No further action is required.

Silicon Graphics also published an advisory for their customers on November 21, 1996--SGI advisory number 19961103-01-I. SGI advisories are available from

http://www.sgi.com/Support/Secur/advisories.html

ftp://sgigate.sgi.com/security/

Sun Microsystems, Inc.

No Sun versions of sendmail are affected by this vulnerability.

Appendix B: anti-smtpd.c

Below is the code for the anti-smtpd.c sendmail wrapper. Here is an example of how to compile and install this wrapper. You may have to change these commands for your system. Further, you may have to change the code for anti-smtpd.c to get it to compile on your system. Finally, you may also have to turn off sendmail before running these commands and then turn sendmail back on after running them. Run these commands as root.

```
# mkdir /usr/hidden
# chmod 700 /usr/hidden
# mv /usr/lib/sendmail /usr/hidden/sendmail
# cc anti-smtpd.c -o anti-smtpd
# mv anti-smtpd /usr/lib/sendmail
# chmod u+s /usr/lib/sendmail
```

Here is the code for anti-smtpd.c:

```
#include <stdio.h>
#include <string.h>
#include <syslog.h>
#include <sysexits.h>

static char *Version = "Version 1.0 November 21, 1996";

/*

**  Sendmail wrapper for CA-96.24 HUP to smtpd problem
```

```
**
**      This is trivial -- it just ensures that sendmail cannot be
**      invoked as smtpd.
**
**      To install this, move the real sendmail into /usr/hidden,
**      which should be a mode 700 directory owned by root. Install
**      this program setuid root in place of sendmail.
*/
#ifndef REAL_SENDMAIL
# define REAL_SENDMAIL  "/usr/hidden/sendmail"
#endif
main(argc, argv)
        int argc;
        char **argv;
{
        char *p;
        extern int errno;
        if (argc < 1)
        {
                fprintf(stderr, "sendmail: need a program name\n");
                exit(EX_USAGE);
        }
        p = strrchr(argv[0], '/');
        if (p == NULL)
                p = argv[0];
        else
                p++;
        if (strcmp(p, "smtpd") == 0 && getuid() != 0)
```

```
        {
                fprintf(stderr, "sendmail: cannot be invoked as
smtpd\n");
                syslog(LOG_ALERT, "sendmail: invoked as smtpd by
%d", getuid());
                exit(EX_USAGE);
        }
        execv(REAL_SENDMAIL, argv);
        fprintf(stderr, "sendmail: cannot exec %s: errno = %d\n",
                REAL_SENDMAIL, errno);
        exit(EX_OSFILE);
}
```

The CERT Coordination Center thanks Eric Allman and AUSCERT for their contributions to the development of this advisory.

Revision History

Sep.24, 1997	Updated copyright statement
May 8, 1997	Appendix A - updated vendor information for Hewlett-Packard.
Nov. 22, 1996	Updates - added vendor information for Silicon Graphics.
	Modified Hewlett Packard's patch information.

25 CA-1996-25: Sendmail Group Permissions Vulnerability

Original issue date: December 10, 1996
Last revised: October 20, 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 security problem in sendmail affecting version 8. By exploiting this vulnerability, a local user can run programs with group permissions of other users. For the exploitation to be successful, group-writable files must be available on the same file system as a file that the attacker can convince sendmail to trust.

The CERT/CC team recommends installing vendor patches or upgrading to the current version of sendmail (8.8.4). Until you can do so, we urge you to apply the workaround provided in Section III.C. In all cases, be sure to take the extra precautions listed in Section III.D.

We will update this advisory as we receive additional information. Please check advisory files regularly for updates that relate to your site. In addition, you can check ftp://ftp.cert.org/pub/latest_sw_versions/sendmail to identify the most current version of sendmail.

I. Description

When sendmail causes mail to be delivered to a program listed in a .forward or :include: file, that program is run with the group permissions possessed by the user who owns that .forward or :include: file. The file's owner attribute is used to initialize the list of group permissions that are in force when the program is run. This list is determined by scanning the /etc/group file, NIS or NIS+ group maps, or other similar vendor-specific databases (such as netinfo on OpenStep).

It is possible for users to obtain group permissions they should not have by linking to a file that is owned by someone else, but on which they have group write permissions. By changing that file, users can acquire the group permissions of the owner of that file.

Exploitation is possible if the attacked user has a file that is group writable by the attacker on the same file system as either (a) the attacker's home directory or (b) an :include: file that is referenced directly from the aliases file and is in a directory writable by the attacker. The first (.forward) attack only works against root. This attack does not give users root "owner" permissions, but does give them access to the groups that list root in /etc/group.

II. Impact

A local attacker can gain the group permissions of another user.

III. Solution

Install a patch from your vendor if one is available (Section A) or upgrade to the current version of sendmail (Section B). Until you can take one of those actions, we recommend applying the workaround described in Section C. In all cases, you should take the precautions described in Section D.

A. Install a vendor patch.

Below is a list of vendors who have provided information about sendmail. Details are in Appendix A of this advisory; we will update the appendix as we receive more information. If your vendor's name is not on this list, please contact the vendor directly.

Berkeley Software Design, Inc. (BSDI)
Cray Research
Digital Equipment Corporation
FreeBSD, Inc.
Hewlett-Packard Company
IBM Corporation
NEC Corporation
The Santa Cruz Operation, Inc. (SCO)
Silicon Graphics Inc
Solbourne (Grumman Support Systems)
Sun Microsystems, Inc.

B. Upgrade to the current version of sendmail.

Install sendmail 8.8.4. This version is a "drop in" replacement for 8.8.x. There is no patch for any version of sendmail before 8.8.0. If you are running such a version, strongly consider moving to version 8.8.4.

Sendmail 8.8.4 is available from

ftp://ftp.sendmail.org/ucb/src/sendmail/sendmail.8.8.4.tar.gz

ftp://ftp.cert.org/pub/tools/sendmail/sendmail.8.8.4.tar.gz

ftp://ftp.cert.dfn.de/pub/tools/net/sendmail/sendmail.8.8.4.tar.gz

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

MD5 (sendmail.8.8.4.tar.gz) = 64ce6393a6968a0dc7c6652dace127b0

Also in that directory are .Z and .sig files. The .Z file contains the same bits as the .gz file, but is compressed using UNIX compress instead of gzip. The .sig is Eric Allman's PGP signature for the uncompressed tar file. The key fingerprint is

```
Type bits/keyID    Date       User ID

pub  1024/BF7BA421 1995/02/23 Eric P. Allman <eric@CS.Berkeley.EDU>
```

```
Key fingerprint =  C0 28 E6 7B 13 5B 29 02  6F 7E 43 3A 48 4F 45 29

                                   Eric P. Allman <eric@Reference.COM>

                                   Eric P. Allman <eric@Usenix.ORG>

                                   Eric P. Allman <eric@Sendmail.ORG>

                                   Eric P. Allman <eric@CS.Berkeley.EDU>
```

When you change to a new version of sendmail, we strongly recommend also changing to the configuration files that are provided with that version. Significant work has been done to make this task easier. (In fact, it is highly likely that older configuration files will not work correctly with sendmail version 8.) It is now possible to build a sendmail configuration file (sendmail.cf) using the configuration files provided with the sendmail release. Consult the cf/README file for a more complete explanation. Creating your configuration files using this method makes it easier to incorporate future changes to sendmail into your configuration files.

Sun sendmail users: A paper is available to help you convert your sendmail configuration files from the Sun version of sendmail to one that works with sendmail version 8.8.x. 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.

C. Apply a workaround.

Eric Allman, the author of sendmail, has provided the following workaround. Note that this workaround is for sendmail 8.8.3. If you are running a version less than 8.8.3 we strongly recommend to upgrade at least to that version (or install the appropriate vendor patches). See CERT advisories CA-95.08 and CA-96.24 for more information on vulnerabilities in older sendmail versions.

Set the UnsafeGroupWrites option in the sendmail.cf file. This option tells sendmail that group-writable files should not be considered safe for mailing to programs or files, causing sendmail to refuse to run any programs referenced from group-writable files. Setting this option is a good idea in any case, but may require your users to tighten permissions on their .forward files and :include: files.

The command "find <filesystem> -user root -type f -perm -020 -print" will print the names of all files owned by root that are group writable on a given file system. While this is only a partial solution we encourage you to carefully check all entries in your alias and .forward files (incl. aliases obtained via NIS, NIS+, or similar information systems) to check for group writable files.

In addition, group memberships should be audited regularly. Users should not be in groups without a specific need. In particular, root generally does not need to be listed in most groups.

As a policy matter, root should have a umask of 022 so that group-writable files are made consciously. Also, the aliases file should not reference :include: files in writable directories.
While checking for writable directories, it's not enough to check the permissions of the directory the file itself lives in. You also have to check all other directories "on top" of that dir. If you, for

example, want to check the permissions of the file
/where/ever/here/file you have to check for group-write permissions not only in the directory /where/ever/here but also check the directories /where/ever and /where.

D. Take additional precautions

Regardless of which solution you apply, you should take these extra precautions to protect your systems. These precautions do not address the vulnerabilities described herein, but are recommended as good practices to follow for the safer operation of sendmail.

- Use the sendmail restricted shell program (smrsh)

With *all* versions of sendmail, use the sendmail restricted shell program (smrsh). You should do this whether you use vendor-supplied sendmail or install sendmail yourself. Using smrsh gives you improved administrative control over the programs sendmail executes on behalf of users.

A number of sites have reported some confusion about the need to continue using the sendmail restricted shell program (smrsh) when they install a vendor patch or upgrade to a new version of sendmail. You should always use the smrsh program.

smrsh is included in the sendmail Version 8 distribution in the subdirectory smrsh. See the RELEASE_NOTES file for a description of how to integrate smrsh into your sendmail configuration file.

smrsh is also distributed with some operating systems.

- Use mail.local

If you run /bin/mail based on BSD 4.3 UNIX, replace /bin/mail with mail.local, which is included in the sendmail distribution. As of Solaris 2.5 and beyond, mail.local is included with the standard distribution. It is also included with some other operating systems distributions, such as FreeBSD.

Although the current version of mail.local is not a perfect solution, it is important to use it because it addresses vulnerabilities that are being exploited. For more details, see CERT advisory CA-95.02.

To use mail.local, replace all references to /bin/mail with /usr/lib/mail.local. If you are using the M4(1)-based configuration scheme provided with sendmail 8.X, add the following to your configuration file:

define(`LOCAL_MAILER_PATH', /usr/lib/mail.local)

- WARNING: Check for setuid executable copies of old versions of mail programs

If you leave setuid executable copies of older versions of sendmail installed in /usr/lib (on some systems, it may be installed elsewhere), the vulnerabilities in those versions could be exploited if an intruder gains access to your system. This applies to sendmail.mx as well as other sendmail programs. Either delete these versions or change the protections on them to be non-executable.

Similarly, if you replace /bin/mail with mail.local, remember to remove old copies of /bin/mail or make them non-executable.

IV. Additional Notes

Three other sendmail vulnerabilities are described in CERT advisory CA-96.20 and CA-96.24; see those advisories for details.

Sendmail 8.8.4 also fixes a denial-of-service attack. If your system relies on the TryNullMXList option to forward mail to third-party MX hosts, an attacker can force that option off, thereby causing mail to bounce. As a workaround, you can use the mailertable feature to deliver to third party MX hosts regardless of the setting of the TryNullMXList option.

Appendix A: Vendor Information

Below is a list of the vendors who have provided information for this advisory. We will update this appendix as we receive additional information. If you do not see your vendor's name, please contact the vendor directly.

Berkeley Software Design, Inc.

BSD/OS is vulnerable to this problem and a patch (U210-030) is available from our mail-back patches server at patches@BSDI.COM or via ftp at ftp://ftp.BSDI.COM/bsdi/patches/patches-2.1/U210-030.

Cray Research

Sendmail version 8 has not been included in any released Unicos system, so this is not a problem for current Unicos systems.

Digital Equipment Corporation

This problem is currently under review by engineering to determine if it impacts DIGITAL UNIX and DIGITAL ULTRIX sendmail implementations.

FreeBSD, Inc.

FreeBSD versions 2.1.5, 2.1.6, and 2.1.6.1 are affected by the group vulnerability. Versions 2.1.6 and 2.1.6.1 are affected by the denial of service vulnerability. All known sendmail security problems will have been addressed prior to the upcoming 2.2 release. Given the complex nature of the patches produced by the sendmail author, user's are encouraged to follow the workarounds described in this advisory or apply and install patches available directly from the author to upgrade to Sendmail 8.8.4 available from the URLs listed in this advisory.

We believe FreeBSD version 2.1.0 and prior to be unaffected by these particular vulnerabilities, however there are significant other security vulnerabilities in the sendmail supplied in prior releases. All FreeBSD users should consider upgrading to sendmail 8.8.4 or removing sendmail

from their systems if they are concerned about unauthorized root access from an unprivileged user account.

Hewlett-Packard Company

Vulnerabilities

1. Sendmail Group Permissions Vulnerability
2. Denial of Service Attack using the sendmail configuration variable TryNullM\XList.

Vulnerable releases

9.x
pre-10.2 10.x
10.2

The 9.x, pre-10.2 10.x sendmail is vulnerable with respect to the "Sendmail Group Permissions Vulnerability".

The 10.2 sendmail is vulnerable with respect to both the reported security holes.

Patches for these vulnerabilities are in progress.

IBM Corporation

The version of sendmail that ships with AIX is vulnerable to the conditions listed in this advisory. A fix is in progress and the APAR numbers will be available soon.

IBM and AIX are registered trademarks of International Business Machines Corporation.

NEC Corporation

Checking out the vulnerability. Contacts for further information by e-mail: UX48-security-support@nec.co.jp.

The Santa Cruz Operation, Inc. (SCO)

Any SCO operating system running a version of sendmail provided by SCO is vulnerable to this problem. SCO will soon be providing a Support Level Supplement, (SLS), to address this issue for the following releases of SCO software:

SCO Internet FastStart release 1.0.0, 1.1.0
SCO OpenServer releases 5.0.0 and 5.0.2

The SLS will provide a version of sendmail release 8.8.4 for these platforms.

Note that only SCO Internet FastStart uses sendmail as the default mail system. All other SCO operating systems use other mail systems such as the Multi-Channel Memorandum Distribution Facility (MMDF) or the "mailsurr" mail system as the default, and as such are not vulnerable to this problem unless otherwise configured to use sendmail.

Please watch the following URLs for availability information:

ftp://ftp.sco.COM/SLS/README

ftp://ftp.sco.COM/SSE/README

Silicon Graphics Inc.

Currently Silicon Graphics Inc does not provide a 8.8.x sendmail version but instead provides a 8.6.12 version. Silicon Graphics has evaluated this issue as possibly applicable to the 8.6.12 version provided by Silicon Graphics and has not found this version to be vulnerable. No further action is required.

Solbourne (Grumman Support Systems)

Solbourne customers running the supported sendmail version

SendMail version 1.1 of 92/11/12 are not vulnerable to this 'denial-of-service' attack.

Those Solbourne customers running later versions of sendmail are probably vulnerable and should consider applying the workaround or installing the latest version of sendmail.

No patches are available.

Sun Microsystems, Inc.

Sun Microsystems has provided the following list of patches in response to this advisory:

```
103594-10 5.5.1

103595-10 5.5.1_86

102980-13 5.5

102981-13 5.5_x86

102066-18 5.4

102064-17 5.4_x86

101739-17 5.3

102423-07 4.1.4

101665-10 4.1.3_U
```

The CERT Coordination Center thanks Eric Allman, AUSCERT, Terry Kyriacopoulos of Interlog Internet Services, and Dan Bernstein of the University of Illinois, Chicago for their contributions to the development of this advisory.

Revision History

Oct. 20, 1997 Appendix A - updated vendor information for Sun.

Sep. 24, 1997 Updated copyright statement

Dec. 20, 1996 Appendix A, Cray - added vendor information.

26 CA-1996-26: Denial-of-Service Attack via ping

Original issue date: December 18, 1996
Last revised: December 5, 1997
Updated information for NCR Corporation.

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

The CERT Coordination Center has received reports of a denial-of-service attack using large ICMP datagrams. Exploitation details involving this vulnerability have been widely distributed.

The CERT/CC team recommends installing vendor patches as they become available.

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 TCP/IP specification (the basis for many protocols used on the Internet) allows for a maximum packet size of up to 65536 octets (1 octet = 8 bits of data), containing a minimum of 20 octets of IP header information and 0 or more octets of optional information, with the rest of the packet being data. It is known that some systems will react in an unpredictable fashion when receiving oversized IP packets. Reports indicate a range of reactions including crashing, freezing, and rebooting.

In particular, the reports received by the CERT Coordination Center indicate that Internet Control Message Protocol (ICMP) packets issued via the "ping" command have been used to trigger this behavior. ICMP is a subset of the TCP/IP suite of protocols that transmits error and control messages between systems. Two specific instances of the ICMP are the ICMP ECHO_REQUEST and ICMP ECHO_RESPONSE datagrams. These two instances can be used by a local host to determine whether a remote system is reachable via the network; this is commonly achieved using the "ping" command.

Discussion in public forums has centered around the use of the "ping" command to construct oversized ICMP datagrams (which are encapsulated within an IP packet). Many ping implementations by default send ICMP datagrams consisting only of the 8 octets of ICMP header information but allow the user to specify a larger packet size if desired.

You can read more information about this vulnerability on Mike Bremford's Web page. (Note that this is not a CERT/CC maintained page. We provide the URL here for your convenience.)

http://www.sophist.demon.co.uk/ping/index.html

II. Impact

Systems receiving oversized ICMP datagrams may crash, freeze, or reboot, resulting in denial of service.

III. Solution

First, since crashing a router or firewall may be part of a larger, multistage attack scenario, we encourage you to inspect the running configuration of any such systems that have crashed to ensure that the configuration information is what you expect it to be.

Then install a patch from your vendor.

Below is a list of vendors who have provided information about patches for this problem. Details are in Appendix A of this advisory; we will update the appendix as we receive more information. If your vendor's name is not on this list, please contact the vendor directly.

Berkeley Software Design, Inc. (BSDI)
Computer Associates, Intl. (products for NCR)
Cray Research
Digital Equipment Corporation
Free BSD, Inc.
Hewlett-Packard Company
IBM Corporation
Linux Systems
NCR Corporation
NEC Corporation
Open Software Foundation (OSF)
The Santa Cruz Operation, Inc. (SCO)
Sun Microsystems, Inc.

Appendix A: Vendor Information

Below is a list of the vendors who have provided information for this advisory. We will update this appendix as we receive additional information. If you do not see your vendor's name, please contact the vendor directly.

Berkeley Software Design, Inc. (BSDI)

BSD/OS 2.1 is not vulnerable to this problem. It correctly handles large packets without any problems.

Computer Associates, Intl.

(products for NCR)

Not vulnerable.

Cray Research

Attempts to send oversized ICMP datagrams are rejected with appropriate error messages. We believe that oversized ICMP datagrams sent to Unicos systems will also be rejected without crashing.

Data General Corporation

Due to the way DG/UX processes tcp packets, DG/UX is not vulnerable to this attack.

Digital Equipment Corporation

MSG ID: SSRT0429 From DSNlink/DIA Database

The following is important information concerning a potential denial of service issue which affects Digital UNIX Operating System, Digital UNIX MLS+, Firewall implementations, and Digital TCP/IP Services for OpenVMS AXP & VAX

```
COMPONENT:  System Security / Potential Denial of Service

DIGITAL UNIX     Version: 3.0, 3.0b, 3.2, 3.2c, 3.2de1, 3.2de2,

                          3.2f, 3.2g, 4.0, 4.0a

DIGITAL UNIX MLS+ Version 3.1a

DIGITAL TCP/IP Services for OpenVMS AXP & VAX Versions - 4.0, 4.1

DIGITAL ULTRIX Versions 4.3, 4.3a, 4.4, 4.5

DIGITAL Firewall for UNIX

DIGITAL AltaVista Firewall for UNIX

DIGITAL VAX/ELN
```

For more information check the DSNlink/DIA Articles (keyword PING), or the URL http://www.service.digital.com/html/whats-new.html for the latest information.

ADVISORY INFORMATION:

Digital recently discovered a potential denial of service issue that may occur by remote systems exploiting a recently published problem while executing the 'ping' command. Solutions and initial communications began appearing in DSNlink/DIA FLASH/articles in late October, 1996.

SEVERITY LEVEL: High.

SOLUTION:

Digital has reacted promptly to this reported problem and a complete set of patch kits are being prepared for all currently supported platforms.

The Digital patches may be obtained from your local Digital support channel or from the URL listed above. Please refer to the applicable README notes information prior to the installation of patch kits on your system.

DIGITAL EQUIPMENT CORPORATION

Free BSD, Inc.

We have fixed the problem in 2.1.6 and -current.

Hewlett-Packard Company

For HP9000 Series 700 and 800 systems, apply the appropriate patch. See Hewlett-Packard Security Bulletin #000040 (HPSBUX9610-040) for further details. The bulletin is available from the HP SupportLine and ftp://ftp.cert.org/pub/vendors/hp/

```
Patch Name(Platform/OS)    | Notes
--------------------------+-------------------------------
PHNE_9027 (s700 9.01)      : PHNE_7704 must first be installed
PHNE_9028 (s700 9.03/5/7)  : PHNE_7252 must first be installed
PHNE_9030 (s700 10.00)     : No patch dependencies
PHNE_9032 (s700 10.01)     : PHNE_8168 must first be installed
PHNE_9034 (s700 10.10)     : PHNE_8063 must first be installed
PHNE_9036 (s700 10.20)     : No patch dependencies
--------------------------+-------------------------------
PHNE_8672 (s800 9.00)      : PHNE_7197 must first be installed
PHNE_9029 (s800 9.04)      : PHNE_7317 must first be installed
PHNE_9031 (s800 10.00)     : No patch dependencies
PHNE_9033 (s800 10.01)     : PHNE_8169 must first be installed
PHNE_9035 (s800 10.10)     : PHNE_8064 must first be installed
PHNE_9037 (s800 10.20)     : No patch dependencies
--------------------------+-------------------------------
```

For our MPE operating system, patches are in process. Watch for the issuance of our MPE security bulletin.

IBM Corporation

See the appropriate release below to determine your action.

AIX 3.2

Apply the following fix to your system:

APAR - IX59644 (PTF - U444227 U444232)

To determine if you have this PTF on your system, run the following command:

```
lslpp -lB U444227 U444232
```

AIX 4.1

Apply the following fix to your system:

APAR - IX59453

To determine if you have this APAR on your system, run the following command:

```
instfix -ik IX59453
```

Or run the following command:

```
lslpp -h bos.net.tcp.client
```

Your version of bos.net.tcp.client should be 4.1.4.16 or later.

AIX 4.2

Apply the following fix to your system:

APAR - IX61858

To determine if you have this APAR on your system, run the following command:

```
instfix -ik IX61858
```

Or run the following command:

```
lslpp -h bos.net.tcp.client
```

Your version of bos.net.tcp.client should be 4.2.0.6 or later.

IBM SNG Firewall

NOTE: The fixes in this section should ONLY be applied to systems running the IBM Internet Connection Secured Network Gateway (SNG) firewall software. They should be applied IN ADDITION TO the IBM AIX fixes listed in the previous section.

IBM SNG V2.1

APAR - IR33376 PTF UR46673

IBM SNG V2.2

APAR - IR33484 PTF UR46641

To Order

APARs may be ordered using Electronic Fix Distribution (via FixDist) or from the IBM Support Center. For more information on FixDist, reference URL: http://service.software.ibm.com/aixsupport/ or send e-mail to aixserv@austin.ibm.com with a subject of "FixDist".

IBM and AIX are registered trademarks of International Business Machines

Linux Systems

We recommend that you upgrade your Linux 1.3.x and 2.0.x kernels to Linux 2.0.27. This is available from all the main archive sites such as ftp://ftp.cs.helsinki.fi/pub/Software/Linux.

Users wishing to remain with an earlier kernel version may download a patch from http://www.uk.linux.org/big-ping-patch. This patch will work with 2.0.x kernel revisions but is untested with 1.3.x kernel revisions.

Red Hat Linux has chosen to issue a 2.0.18 based release with the fix. Red Hat users should obtain this from ftp://ftp.redhat.com/pub/redhat/redhat-4.0/updates/i386/kernel-2.0.18-6.i386.rpm.

NCR Corporation

For MP-RAS 3.00 and above, using TCP/IP as package name "inet", not vulnerable.

NEC Corporation

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	not vulnerable
UP-UX/V	R1.x - R4.x	not vulnerable
UP-UX/V(Rel4.2MP)	R5.x - R7.x	not vulnerable
UX/4800	R11.x	not vulnerable

NCR

see Computer Associates, Intl.

Open Software Foundation (OSF)

OSF's OSF/1 R1.3.3 maintenance release includes a solution for this problem.

The Santa Cruz Operation, Inc. (SCO)

The following SCO products are known to be vulnerable:

SCO OpenServer 5.0.0, 5.0.2
SCO Internet FastStart 1.0.0, 1.1.0
SCO Open Desktop 3.0
SCO TCP/IP 1.2.1 on SCO Unix System V/386 Release 3.2 Version 4.2

The symptoms encountered vary greatly and seem to be related to the type of network interface device being used. Support Level Supplement (SLS) OSS449 addresses this problem for the following releases:

SCO OpenServer 5.0.0, 5.0.2
SCO Internet FastStart 1.0.0, 1.1.0.

This Supplement is available at the following URLs:

ftp://ftp.sco.COM/SLS/oss449a.ltr (cover letter)
ftp://ftp.sco.COM/SLS/oss449a.Z (image)

The checksums are as follows:

```
sum -r

  ------

        oss449a.ltr:    28877   42

          oss449a.Z:    54558 1762

  MD5

  ---

        MD5 (oss449a.Z) = e8fc8a29dd59683ce5107f3b9b8d1169

        MD5 (oss449a.ltr) = d51ee1caf33edb86f4dbeb1733c99d86
```

If this SLS is ever updated, it will be noted at ftp://ftp.sco.COM/SLS/README.

Should more information become available for either SCO's OpenServer or UnixWare products, SCO will provide updated information for this advisory.

If you need further assistance, SCO's Web page is at http://www.sco.COM.

Support requests from supported customers may be addressed to support@sco.COM , or you may contact SCO as follows:

USA/Canada: 6am-5pm Pacific Standard Time (PST)
1-408-425-4726 (voice)
1-408-427-5443 (fax)

Pacific Rim, Asia, and Latin American customers: 6am-5pm Pacific Standard Time (PST)
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)

Sun Microsystems, Inc.

Sun Microsystems has provided the following list of patches in response to this advisory:

```
103630-09 5.5.1

103631-09 5.5.1_x86

103169-12 5.5

103170-12 5.5_x86

101945-51 5.4

101946-45 5.4_x86
```

The CERT Coordination Center staff thanks AUSCERT, the Australian Computer Emergency Response Team, and DFN-CERT, the German team, for their contributions to this advisory, and we thank Mike Bremford for permission to cite the information he has made available to the community.

Revision History

```
Dec. 5, 1997  Appendix A - Updated information for NCR Corporation.

Sep. 24,1997  Updated copyright statement

Aug. 7, 1997  Changed vendor information for Sun Microsystems to re-
move incorrect patch reference.

July 28, 1997 Added vendor information for Sun Microsystems.
```

Jan. 20, 1997 Appendix A - added information from Data General Corporation.

Jan. 14, 1997 Appendix A - modified SCO entry to include updated patch information.

27 CA-1996-27: Denial-of-Service Attack via ping

Original issue date: December 19, 1996
Last revised: September 24, 1997
Updated copyright statement

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

The text of this advisory was originally released on October 11, 1996, as AA-96.04.Vulnerability.in.HP.Software.Installation.Programs, developed by AUSCERT. Because of the seriousness of the problem, we are reprinting the AUSCERT advisory here with their permission. Only the contact information at the end has changed: AUSCERT contact information has been replaced with CERT/CC contact information.

We will update this advisory as we receive additional information. Look for it in an "Updates" section at the end of the advisory.

AA-96.04
AUSCERT Advisory

Vulnerability in HP Software Installation Programs
11 October 1996

AUSCERT has received information that there is a vulnerability in the Hewlett Packard Software Distributor product, SD-UX, used to install, update, remove and package HP-UX software and patches. This software is installed by default under HP-UX 10.x and may have been specifically installed as additional software under HP-UX 9.x. Any system with the SD-UX package installed is vulnerable.

This vulnerability may allow local users to gain root privileges.

Exploit details involving this vulnerability have been made publicly available.

Vendor patches are being developed, but until they are made available, AUSCERT recommends that sites take the actions suggested in Section 3.

1. Description

The HP Software Distributor (SD-UX) is a package that provides a user interface which can be used to install, update, remove, and package HP-UX software and patches.

The programs supplied with this package create files in an insecure manner. As these programs execute with root privileges, it is possible to create or over-write arbitrary files on the system. The default location of the programs supplied by the package is /usr/sbin.

To determine if you have SD-UX installed on your system, check for the presence of the swinstall (and related) files using the following command:

```
% ls -l /usr/sbin/sw*
```

Individual sites are encouraged to check their systems for the SD-UX package, and if installed, take the actions recommended in Section 3.

2. Impact

Local users may be able to create or over-write arbitrary files on the system. This can be leveraged to gain root privileges.

3. Workarounds/Solution

AUSCERT recommends that sites prevent possible exploitation of this vulnerability by taking the measures stated in Section 3.1 immediately.

If software maintenance is required, AUSCERT advises that sites use one of the workarounds given in 3.2, preferably that described in Section 3.2.1.

Vendor patches may also address this vulnerability in the future (Section 3.3).

3.1 Remove permissions

Until official patches are available sites are encouraged to completely prevent the execution of all vulnerable SD-UX programs by any user (including root).

```
# chmod 400 /usr/sbin/swinstall
# chmod 400 /usr/sbin/swmodify
```

Note that if only the setuid permissions are removed, it is still possible for users to gain the privileges of any user executing the SD-UX programs (including root).

3.2 Workarounds

AUSCERT recommends that if software maintenance is required, sites implement one of the following workarounds until official vendor patches are made available.

The workaround described in 3.2.1 is the preferred method of doing software maintenance. If sites are unable to bring their machines into single user mode, the workaround given in Section 3.2.2 may be more applicable.

3.2.1 Run in single user mode

If packages must be installed, the machine should be brought into single-user mode, execute permissions re-enabled on /usr/sbin/swinstall,

```
# chmod 700 /usr/sbin/swinstall
# chmod 700 /usr/sbin/swmodify
```

and all symbolic links in /var/tmp and /tmp removed. The following command can be used to remove the symbolic links:

```
# find /tmp /var/tmp -type l -ok rm {} \;
```

Once this has been completed, any software package maintenance may be safely performed.

The execute permissions on the vulnerable programs must be removed before the machine is brought back into multi-user mode.

```
# chmod 400 /usr/sbin/swinstall
# chmod 400 /usr/sbin/swmodify
```

3.2.2 Change temporary file environment variable

This workaround should only be used if the SD-UX programs must be used while the machine is in multi-user mode.

The SD-UX programs use a number of temporary files. The location of these files can be configured using the environment variable TMPDIR. It is possible to set the environment variable TMPDIR to a non-world writable directory. Having the temporary files created in a non-world writable directory prevents the exploitation of the vulnerability described in this advisory.

NOTE: The environment variable must be set in each login session BEFORE any SD-UX programs are used.

To use this method, the following steps must be taken:

1. As root, create a non-world writable temporary directory for the temporary files used by the SD-UX programs. The location of these temporary files can be configured with the TMPDIR environment variable. In this workaround, we have chosen to use the directory /var/tmp/SD_tmp.

   ```
   # mkdir /var/tmp/SD_tmp
   # chmod 700 /var/tmp/SD_tmp
   ```

   For this workaround to be effective, sites should ensure that the parent directory of $TMPDIR has the sticky bit set if the parent directory is world writable. In this workaround, /var/tmp is the directory concerned. The sticky bit on /var/tmp can be set with the command:

   ```
   # chmod 1777 /var/tmp
   ```

   In all sessions where software maintenance is performed:

2. Change permissions on the vulnerable programs:

   ```
   # chmod 700 /usr/sbin/swinstall
   # chmod 700 /usr/sbin/swmodify
   ```

3. Set the environment variable TMPDIR:

   (under csh)
   # setenv TMPDIR /var/tmp/SD_tmp

   (under sh)
   # TMPDIR=/var/tmp/SD_tmp; export TMPDIR

   and verify that the directory exists and is writable by root.

   # ls -ld $TMPDIR

4. Perform any software package maintenance.

5. Remove the execute permissions on the vulnerable programs:

   # chmod 400 /usr/sbin/swinstall
   # chmod 400 /usr/sbin/swmodify

6. The environment variable TMPDIR is used by many other programs. You should either exit this interactive session, or reset the TMPDIR environment variables before continuing.

   NOTE: Steps 2) through 6) must be repeated each time software maintenance is performed.

3.3 Install vendor patches

Official vendor patches are currently being developed to address the vulnerability described in this advisory. When vendor patches are made available, AUSCERT suggests that they be installed.

AUSCERT thanks Information Technology Services of the University of Southern Queensland, Viviani Paz (The University of Queensland) and Hewlett Packard for their assistance in this matter.

UPDATES

Hewlett-Packard

Information concerning patches for the vulnerability described in this advisory can be found in HEWLETT-PACKARD SECURITY BULLETIN, "Security Vulnerability in swinstall command," Document ID: HPSBUX9707-064

1) From your Web browser, access the URL: http://us-support.external.hp.com (for US,Canada, Asia-Pacific, and Latin-America) or http://europe-support.external.hp.com (for Europe).

2) On the HP Electronic Support Center main screen, select the hyperlink "Support Information Digests".

3) On the "Welcome to HP's Support Information Digests" screen, under the heading "Register Now", select the appropriate hyperlink "Americas and Asia-Pacific", or "Europe".

4) On the "New User Registration" screen, fill in the fields for the User Information and Password and then select the button labeled "Submit New User".

5) On the "User ID Assigned" screen, select the hyperlink "Support Information Digests".

Note what your assigned user ID and password are for future reference.

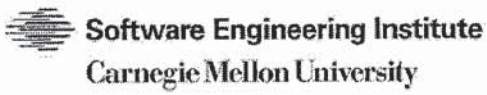
6) You should now be on the "HP Support Information Digests Main" screen. You might want to verify that your email address is correct as displayed on the screen. From this screen, you may also view/subscribe to the digests, including the security bulletins digest.

To get a patch matrix of current HP-UX and BLS security patches referenced by either Security Bulletin or Platform/OS, click on following screens in order:

Technical Knowledge Database
Browse Security Bulletins
Security Bulletins Archive
HP-UX Security Patch Matrix

Revision History

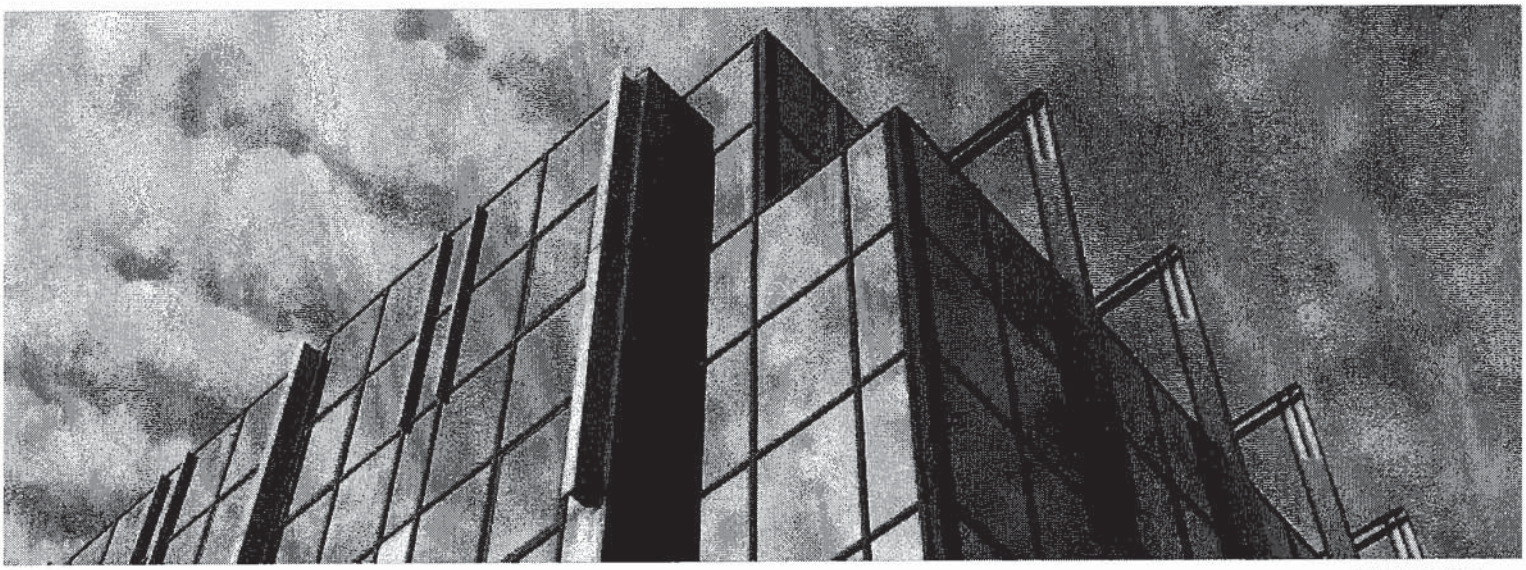
```
Sep. 24, 1997  Updated copyright statement

July 28, 1997 Updates section - added information from Hewlett-Pack-
ard.
```



1996 CERT Advisories

CERT Division

http://www.sei.cmu.edu



REV-03.18.2016.0

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

This report was prepared for the

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

DM17-0052

Table of Contents

Digital Library

White Paper

1996 CERT Advisories

December 1996

This document contains the CERT advisories from 1996.

Vulnerability Analysis

Publisher: CERT Division

Abstract

CERT/CC advisories are now part of the US-CERT National Cyber Awareness System. We provide these advisories, published by year, for historical purposes.

Download

Ask a question about this White Paper

Back to Top

Connect with Us

Contact Us

4500 Fifth Avenue
Pittsburgh, PA 15213-2612
U.S.A.
412-268-5800

Who We Are

The Software Engineering Institute (SEI) is a federally funded research and development center (FFRDC) sponsored by the U.S. Department of Defense (DoD). It is operated by Carnegie Mellon University.

About

Leadership
News
Calendar of Events
Year in Review
Careers
Locations

Services

Engage with Us
Partner Network
SEI Training

Work Areas

Acquisition Support
Cyber-Physical Systems
Measurement & Analysis
Performance & Dependability
Pervasive Mobile Computing
Process & Performance Improvement
Risk Management
Security & Survivability
Smart Grid
Software Architecture
Software Product Lines
System of Systems
Ultra-Large-Scale Systems

Resources

Insights
Digital Library
Podcasts
Webinars
Tools & Methods
Legal

SEI INSIGHTS

Simultaneous Analysis of Safety and Security of a Critical System

By Sam Procter

September 11, 2017

LATEST WEBINAR

Five Keys to Effective Agile Test Automation for Government Programs

By Robert Binder , Suzanne Miller

August 25, 2017