CERT Advisory CA-1995-14 Telnetd Environment Vulnerability

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

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

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

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

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

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

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

I. Description

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

Users with accounts on the targeted system can exploit this vulnerability. Users without accounts on that system can also exploit this vulnerability if they are first able to deposit an altered shared object library onto the targeted system. Therefore, a system may be vulnerable to users with and without local accounts.

Not all systems that run an RFC 1408/RFC 1572-compliant telnet daemon and support shared object libraries are vulnerable. Some vendors have changed the trust model such that environment variables provided by the telnet daemon are not trusted and therefore are not used by the login program. Section III contains a summary of information vendors have reported as of the date of this advisory.

II. Impact

Local and remote users can become root on the targeted system.

III. Solution

The general solution to this problem is to replace the telnet daemon with one that changes the environment given to the login program. We recommend that you install a patch from your vendor if possible. If this is not possible, we recommend using the workaround in Appendix B until you can install a patch. Finally, if you have previously installed Mr. Borman's telnet package, see Section C for how to get a new version that fixes the vulnerability.

A. Vendor Patches

Below is a summary of the vendors listed in Appendix A of this advisory. More complete information, including how to obtain patches, is provided in the appendix. We will update the appendix as we receive more information from vendors.

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

REMINDER: If you installed a version of David Borman's telnet package that is older than October 23, 1995, your system may be vulnerable even though it was not vulnerable as distributed by the vendor.

Vendor or Source

Apple Computer
Berkeley Software Design
Cray Research
CYGNUS
Data General
Digital Equipment
FreeBSD
Harris
Hewlett-Packard
IBM Corp.
Linux
MIT-distributed for Athena
NEC
NetBSD
Open Software Foundation
OpenVision
SCO
SGI
Sony Corp.

B. Workaround

Until you can install a patch from your vendor, you can use the workaround provided in Appendix B.

C. If you have installed a previous version of Mr. Borman's telnet package, note that he has fixed this problem in the version available at the following location:

ftp://ftp.cray.com/src/telnet/telnet.95.10.23.NE.tar.Z
MD5 checksum 2e14879a5b0aa6dd855a17fa8a3086cf

Appendix A: Vendor Information

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

Apple Computer, Inc.

Apple's A/UX is not vulnerable.

Berkeley Software Design, Inc.

BSDI's BSD/OS is not vulnerable.

Cray Research, Inc.

Cray's UNICOS is not vulnerable.

CYGNUS Network Security V4 Free Network Release

cns-95q1 is vulnerable. cns-95q4 is not vulnerable.

Customers can use the following URL to obtain the patch:

http://www.cygnus.com/data/cns/telnetdpatch.html

If customers are unable to obtain the patch in this manner
or have any questions, send e-mail to kerbask@cygnus.com

Note that while the URL and patch are already available, there is no link to the page yet. We will add a link once the announcement has been made.

Data General Corporation

Data General believes the DG/UX operating system to be NOT vulnerable to this problem. This includes all supported releases, DG/UX 5.4 Release 3.00, DG/UX 5.4 Release 3.10, DG/UX Release 4.10 and all related Trusted DG/UX releases.

Specifically, telnetd shipped in DG/UX does not support environment options and does not support RFC 1572.

Digital Equipment Corporation

Digital's OSF/1: vulnerable
Digital's ULTRIX: not vulnerable

Digital has corrected this potential vulnerability. Patches containing new images for Digital's OSF/1 platforms are being provided to your normal Digital Support channels beginning October 31 (U.S. time). The kits may be identified as ECO SSRT0367 (telnetd) for DEC OSF/1 V2.0 thru V3.2c

This potential vulnerability is not present on Digital's ULTRIX systems.

Digital distribution of this announcement will be via AES services (DIA, DSNlink FLASH etc.). Digital Equipment Corporation strongly urges Customers to upgrade to a minimum of DEC OSF/1 V3.0, then apply this patch.

FreeBSD

Vulnerable. A patch has been applied to the current development FreeBSD source tree which is not yet released. This patch is slightly modified compared to posted one, i.e. only variables which affects FreeBSD are disabled. It is telnetd patch, not a login wrapper.

For the official patch, location please contact:

Jordan Hubbard <jkh@FreeBSD.org>

Harris

Harris Computer Systems Corporation's Night Hawk is not vulnerable.

Hewlett-Packard Company

HP/UX is not vulnerable.

IBM Corporation

AIX is not vulnerable to this attack.

Linux (freely available software; not a vendor)

Debian GNU/Linux (From "Peter Tobias" <tobias@et-inf.fho-emden.de>):
The current version of the Debian GNU/Linux distribution (released 10/27/95) is not vulnerable anymore. All Debian Installations that use a netstd package version prior to v1.21-1 are vulnerable (telnetd is part of the netstd package). netstd-1.21-1 and above are ok.

Patches are available. Peter fixed the bug last week and uploaded the fixed version to our ftp site (ftp.debian.org). Binaries, sources and the diffs against the bsd telnetd can be found there. The URL for the new binary package is:

ftp://ftp.debian.org/debian/debian-0.93/binary/net/netstd-1.21-1.deb

and the sources and the diff against the bsd telnetd can be found at:

ftp://ftp.debian.org/debian/debian-0.93/source/net/netstd-1.21-1/telnetd.tar.gz
ftp://ftp.debian.org/debian/debian-0.93/source/net/netstd-1.21-1/telnetd.diff.gz

Red Hat Linux (From Erik Troan <ewt@redhat.com>):
Vulnerable. A fix is now available at:

ftp://ftp.redhat.com/pub/redhat-2.0/updates/NetKit-B-0.06-4.i386.rpm
ftp://ftp.pht.com/pub/linux/redhat/redhat-2.0/updates/NetKit-B-0.06-4.i386.rpm

It will also be fixed in the upcoming Red Hat 2.1 release.

Slackware Linux is vulnerable. The fixes are available from:

ftp://ftp.cymru.net/pub/linux/security/in.telnetd.bin.gz
MD5 (in.telnetd.bin.gz) = 300fc2b022f338e32db411d0e14f0bed

ftp://ftp.cymru.net/pub/linux/security/in.telnetd.bin.elf.gz
MD5 (in.telnetd.bin.elf.gz) = a9ed9a0b90b7a62c98c185e9c7970c5e

The CERT Coordination Center has received information that Paul Leyland <plc@sable.ox.ac.uk> has placed patches for Linux on ftp.ox.ac.uk.

Non-US sites may want to obtain the patches from this archive for convenience. However, please note that these patches will only be available for the next few months; at some point they will be removed from this location.

Linux: This consists of a README, a patch for the telnetd source and a compiled telnetd which should be ok for most Slackware distributions and is available from

ftp://ftp.ox.ac.uk/pub/comp/security/software/patches/telnetd/linux

MD5 (envpatch) = 3dff044bae0ee7076b8dce735e174962
MD5 (telnetd) = ee2146342059ab00b94fae19f9b1ea63
MD5 (README) = 83f8d07a9b9e8f307346d2ac4b8b3f39

MIT-distributed Athena telnet/telnet95

Vulnerable. Patches available in:
ftp://aeneas.mit.edu/pub/kerberos/telnet-patch/

beta4-3.patch is the patch versus the Beta 4 patch level 3 distribution of Kerberos v5.

beta5.patch is the patch versus the Beta 5 distribution of Kerberos V5.

Both patches have been PGP signed by Ted Ts'o <tytso@MIT.EDU> using detached signatures (beta4-3.patch.sig and beta5.patch.sig).

NEC Corporation

Some NEC systems are vulnerable. Here is their vulnerability matrix:

```
       OS                Version        Status
- ------------------   ------------   -------------------------------------
EWS-UX/V(Rel4.0)     R1.x - R6.x    not vulnerable

EWS-UX/V(Rel4.2)     R7.x - R10.x   not vulnerable

EWS-UX/V(Rel4.2MP)   R10.x          vulnerable
                                    patch available

UP-UX/V              R2.x - R4.x    not vulnerable

UP-UX/V(Rel4.2MP)    R5.x - R7.x    vulnerable
                                    patch available

UX/4800              R11.x          vulnerable
                                    patch available
```

The patches are available through anonymous FTP from ftp://ftp.meshnet.or.jp in the /pub/48pub/security directory. Please refer to the README file in the directory concerning the appropriate patches that should be retrieved.

```
          OS          Version                Patch-ID and Checksums
  ------------------ ------- -------------------------------------------------
   EWS-UX/V(Rel4.2MP)  R10.x  NECmas001
                              Results of sum = 760 295
                  MD5 (NECmas001.COM.pkg)   = 588ED562BBDA6AFF45F1910A75C19B30

   UP-UX/V(Rel4.2MP)   R5.x   NECu5s001
                              Results of sum = 22675 293
                  MD5 (NECu5s001.COM.pkg)   = CBBA695079570BE994EDE8D5AD296B38

                       R6.x   NECu6s001
                              Results of sum = 40159 293
                  MD5 (NECu6s001.COM.pkg)   = C891AF03402CFD092B930253DC3CD607

                       R7.x   NECu7s001
                              Results of sum = 65094 295
                  MD5 (NECu7s001.COM.pkg)   = 00BAFAFF4A8FCFFB58FB6F8F94039D14

   UX/4800             R11.x  NECmbs002
                              Results of sum = 34536 295
                  MD5 (NECmbs002.COM.pkg)   = E6ADAAC22C1B32C4180B855C19B49205
```

Contacts for further information:

Email: UX48-security-support@nec.co.jp

NetBSD

NetBSD 1.0 (the last official release) is vulnerable; NetBSD 1.1 (due out in mid-November) will not be. NetBSD-current is not vulnerable, as of a week or so ago.

Patches: A source form patch has been developed. A core team member will have to make source and binary patches available and provide a location for it.

The login-wrapper given in the advisory can be compiled with NetBSD with:

```
cc -static -o login-wrapper login-wrapper.c
```

Open Software Foundation

OSF/1 version 1.3 is not vulnerable.

OpenVision

This is from: Barry Jaspan <bjaspan@cam.ov.com>:
OpenVision has a patch for the telnetd in OpenV*Secure 1.2 and will contact its customers directly.

The Santa Cruz Operation Inc.

SCO is NOT vulnerable.

Silicon Graphics

On November 16, 1995, Silicon Graphics updated their advisory, 19951101-02-P1010o1020, concerning the Telnetd vulnerability.

In the original advisory, 19951101-01-P1010o1020, the patches 1010 and 1020 were indicated for the wrong versions of IRIX. Patch 1010 is for IRIX 6.1 and patch 1020 is for IRIX 5.2, 5.3, 6.0, 6.0.1. The corrections have been made below.

The solution for this issue is a replacement of the telnetd program for those versions that are vulnerable. The following patches have been generated for those versions vulnerable and freely provides them for the community.

IRIX 3.x

This version of IRIX is not vulnerable. No action is required.

IRIX 4.x

This version of IRIX is not vulnerable. No action is required.

IRIX 5.0.x, 5.1.x

For the IRIX operating systems versions 5.0.x, 5.1.x, an upgrade to 5.2 or better is required first. When the upgrade is completed, then the patches described in the next sections "**IRIX 5.2, 5.3, 6.0, 6.0.1, 6.1**" or "**IRIX 6.1**" can be applied.

IRIX 5.2, 5.3, 6.0, 6.0.1

For the IRIX operating system versions 5.2, 5.3, 6.0, and 6.0.1, an inst-able patch has been generated and made available via anonymous ftp and/or your service/support provider. The patch is number 1020 and will install on IRIX 5.2, 5.3, 6.0 and 6.0.1 .

The SGI anonymous ftp site is sgigate.sgi.com (204.94.209.1). Patch 1020 can be found in the following directories on the ftp server:

> ~ftp/Security
>
> or
>
> ~ftp/Patches/5.2
> ~ftp/Patches/5.3
> ~ftp/Patches/6.0
> ~ftp/Patches/6.0.1

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

```
Filename:                 README.patch.1020
Algorithm #1 (sum -r):    31057 8 README.patch.1020
Algorithm #2 (sum):       40592 8 README.patch.1020
MD5 checksum:             02F06ECD6240015F8DF82A99EC01E911

Filename:                 patchSG0001020
Algorithm #1 (sum -r):    07232 2 patchSG0001020
Algorithm #2 (sum):       47310 2 patchSG0001020
MD5 checksum:             DA2341626FAEB9D67BA85FA3465BA9D9

Filename:                 patchSG0001020.eoe1_sw
Algorithm #1 (sum -r):    22449 62 patchSG0001020.eoe1_sw
Algorithm #2 (sum):       36518 62 patchSG0001020.eoe1_sw
MD5 checksum:             936019F2CC9AB6CAE0D2DF611D461475

Filename:                 patchSG0001020.eoe2_sw
Algorithm #1 (sum -r):    29899 43 patchSG0001020.eoe2_sw
Algorithm #2 (sum):       12088 43 patchSG0001020.eoe2_sw
MD5 checksum:             19A9C0BCB6F178E7EDF86850A1CF81D1

Filename:                 patchSG0001020.idb
Algorithm #1 (sum -r):    64615 2 patchSG0001020.idb
Algorithm #2 (sum):       46761 2 patchSG0001020.idb
MD5 checksum:             487831A62C61FEAF5797859CBC1F018C
```

IRIX 6.1

For the IRIX operating system version 6.1, an inst-able patch has been generated and made available via anonymous ftp and/or your service/support provider. The patch is number 1010 and will install on IRIX 6.1 .

The SGI anonymous ftp site is sgigate.sgi.com (204.94.209.1). Patch 1010 can be found in the following directories on the ftp server:

~ftp/Security

or

~ftp/Patches/6.1

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

```
Filename:                 README.patch.1010
Algorithm #1 (sum -r):    43949 8 README.patch.1010
Algorithm #2 (sum):       38201 8 README.patch.1010
MD5 checksum:             A8781E18A1F79716FBFE0B6E083DAB31

Filename:                 patchSG0001010
Algorithm #1 (sum -r):    08656 2 patchSG0001010
Algorithm #2 (sum):       45506 2 patchSG0001010
MD5 checksum:             34CF7F63073C225AD76150A4088E76AB

Filename:                 patchSG0001010.eoe1_sw
Algorithm #1 (sum -r):    12843 65 patchSG0001010.eoe1_sw
Algorithm #2 (sum):       42034 65 patchSG0001010.eoe1_sw
MD5 checksum:             82B8D375ECBF58A08286D393CE3980E7

Filename:                 patchSG0001010.eoe2_sw
Algorithm #1 (sum -r):    01655 47 patchSG0001010.eoe2_sw
Algorithm #2 (sum):       19507 47 patchSG0001010.eoe2_sw
MD5 checksum:             1A5C5B5B84E0188A923C48419F716492

Filename:                 patchSG0001010.idb
Algorithm #1 (sum -r):    31514 2 patchSG0001010.idb
Algorithm #2 (sum):       46531 2 patchSG0001010.idb
MD5 checksum:             9540492FEB00D41281AAF90AC3F67FA9
```

SGI Security Information/Contacts:

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

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

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

Sony Corporation

Sony's NEWS-OS 6.x is not vulnerable.

Sun Microsystems, Inc.

Versions of Solaris prior to 2.5 and SunOS do not support the "environ" option and are not affected by the reported problem.

Appendix B: login-wrapper Workaround

The login-wrapper program shown below is meant to be executed just before the distributed login program. The wrapper cleans specific variables from the environment before invoking the distributed login program.

```
- ------------------------cut here--8<------------------------
/*
 * This is a login wrapper that removes all instances of
 * various variables from the environment.
 *
 * Note: this program must be compiled statically to be
 * effective against exploitation.
 *
 * Author:      Lawrence R. Rogers
 *
 * 10/25/95     version 1.1     Original version
 * 10/26/95     version 1.2     ELF_ variables removed (Linux)
 * 10/27/95     version 1.3     ELF_ changed to ELF_LD_
 *                              Added AOUT_LD_ (Linux)
 *
 */

#include        <stdio.h>

#if !defined(_PATH_LOGIN)
# define                _PATH_LOGIN     "/bin/login.real"
#endif

main (argc, argv, envp)
int argc;
char **argv, **envp;
{
        register char **p1, **p2;

        for (p1 = p2 = envp; *p1; p1++) {
                if (strncmp(*p1, "LD_", 3) != 0 &&
                    strncmp(*p1, "_RLD", 4) != 0 &&
                    strncmp(*p1, "LIBPATH=", 8) != 0 &&
                    strncmp(*p1, "ELF_LD_", 7) != 0 &&
                    strncmp(*p1, "AOUT_LD_", 8) != 0 &&
                    strncmp(*p1, "IFS=", 4) != 0 ) {
                            *p2++ = *p1;
                }
        }
        *p2 = 0;
        execve(_PATH_LOGIN, argv, envp);
        perror(_PATH_LOGIN);
        exit(1);
}
- ------------------------cut here--8<------------------------
```

The following two examples show how to compile the login-wrapper for SGI's IRIX 5.3 and FreeBSD 2.x systems. The examples move the distributed login program to a new location and install the wrapper in the standard location. When executed, the wrapper first cleanses the environment and then calls the relocated, distributed login program.

Note 1: The wrapper must be compiled statically. On SGI's IRIX system, compiling statically requires that the non-shared versions of libraries be installed. Consult your system documentation to determine how to do this.

Note 2: You may need to change the _PATH_LOGIN variable to define where the real login program resides on your system. On some systems, login resides in /usr/bin/login.

Compiling for IRIX 5.3

```
# uname -a
IRIX test 5.3 11091812 IP22 mips
# /bin/ls -l /usr/lib/iaf/scheme
- -rwsr-xr-x    1 root     sys        65832 Sep  9 14:24 /usr/lib/iaf/scheme
# /bin/cc -non_shared -O -D_PATH_LOGIN=\"/usr/lib/iaf/scheme.real\" \
        login-wrapper.c -o login-wrapper
# /bin/mv /usr/lib/iaf/scheme /usr/lib/iaf/scheme.real
# /bin/chmod 755 /usr/lib/iaf/scheme.real
# /bin/mv login-wrapper /usr/lib/iaf/scheme
# /bin/chmod 4755 /usr/lib/iaf/scheme
# /bin/chown root /usr/lib/iaf/scheme
# /bin/chgrp  sys /usr/lib/iaf/scheme
# /bin/ls -lL /usr/lib/iaf/scheme /usr/lib/iaf/scheme.real
- -rwxr-xr-x    1 root     sys        65832 Sep  9 14:24
/usr/lib/iaf/scheme.real
- -rwsr-xr-x    1 root     sys       213568 Oct 30 08:42 /usr/lib/iaf/scheme
```

Compiling for FreeBSD 2.x

```
# /bin/ls -lg /usr/bin/login
- -r-sr-xr-x  1 root  bin  20480 Jun 10 20:00 /usr/bin/login
# /usr/bin/cc -D_PATH_LOGIN=\"/usr/bin/login.real\" -static \
        -O login-wrapper.c -o login-wrapper
# /bin/mv /usr/bin/login /usr/bin/login.real
# /bin/chmod 555 /usr/bin/login.real
# /bin/mv login-wrapper /usr/bin/login
# /bin/chmod 4555 /usr/bin/login
# /usr/sbin/chown root.bin /usr/bin/login
# /bin/ls -lg /usr/bin/login /usr/bin/login.real
- -r-sr-xr-x  1 root  bin  24885 Oct 25 22:14 /usr/bin/login
- -r-xr-xr-x  1 root  bin  20480 Jun 10 20:00 /usr/bin/login.real
```

The CERT Coordination Center staff thanks Eric Halil of AUSCERT, Wolfgang Ley of DFNCERT, and Sam Hartman of the MIT Kerberos Development team for their support in responding to this problem.

Revision History

```
Oct. 30, 1997  Updated vendor information for Sun.
Sep. 26, 1997  Updated copyright statement
Aug. 30, 1996  Information previously in the README was inserted
               into the advisory.
Mar. 22, 1996  Appendix A, SGI -  Modified information for Silicon Graphics.
Feb. 08, 1996  Appendix A, NEC -  Added patch information.
Nov. 08, 1995  Appendix A, IBM - Added an entry for IBM.
                          Linux - Added information about Slackware Linux.
                          NetBSD - Corrected compilation instructions.
                          SCO - Noted SCO is not vulnerable.
                          SGI - Updated information.
                          Sun - Added an entry.
Nov. 08, 1995  Appendix B - Replaced IRIX 5.3 section with new material.
```