CERT Advisory 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 back-slashes.

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