CERT Advisory CA-1995-13 Syslog Vulnerability - A Workaround for Sendmail

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

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

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

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

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

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

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

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

I. Description

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

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

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

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

II. Impact

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

III. Solution

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

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

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

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

B. Install sendmail version 8.7.1.

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

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

Sendmail is available by anonymous FTP from

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

Checksum:

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

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

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

C. Install smrsh.

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

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

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

IV. Building this package for SunOS 4.1.X

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

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

See Section VI for final installation steps.

V. Building this package for Solaris 2.X

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

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

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

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

VI. Final Installation Notes

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

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

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

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

Appendix A: Vendor Information

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

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

Eric Allman

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

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

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

Berkeley Software Design, Inc.

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

md5 checksum: 88b3fd8c83a5926589d7b87b55bc4e14
```

Convex Computer Corporation

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

Vulnerable:  ConvexOS (all releases)
             SPPUX (all releases)

A patch is being developed to address this vulnerability in currently
supported releases as detailed below.  Contact the Convex Technical
Assistance Center 1-800-952-0379 to obtain information and patches.

There are no known automated attack programs in existence for Convex or
SPP architectures.  Development of such a program would require access
to such a machine, as well as detailed knowledge of the architecture.
However, the only completely secure work-around at this time would be to
disable sendmail (known to have been successfully attacked on other
architectures), as well as other daemons which can potentially log
user-supplied strings.  Note that the user-supplied strings do not have
to actually be routed by syslogd in order for this vulnerability to
occur.  At this time we do not have a canonical list of affected
software; sendmail is the only known-vulnerable agent.

It should also be noted that Convex machines make use of a "SPU"
workstation (also referred to as a "test station") which controls the
machine; these workstations are vulnerable if sendmail is enabled on
those workstations and the SPU or test station is located on an
accessible network.  Convex recommends disabling sendmail on SPU and
test-station workstations until a patch can be obtained from Convex.

Currently supported OS releases as of Sep 1, 1995:

        ConvexOS 10.1, 10.2, 11.0, 11.1
        SPPUX    3.x
```

Cray Research

Information about fixes for the syslog problem can be found in FN #2011, dated October 10, 1995. Customers should receive this information from their Cray Research service representative.

For all source installations, your Cray Research service representative can obtain the fix via the getfix tool.

Due to the number of executables which use this library routine, it is not possible to provide getfix packages for all binary installations. UNICOS binary update packages 8.0.4.2 and 9.0.1.2 include this mod.

FIX AVAILABILITY as of Feb. 1996

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

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

Data General Corporation

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

Digital Equipment Corporation

For updated information, please refer to the Digital Equipment Corporation Vendor Bulletin #96.0383, available in

ftp://ftp.cert.org/pub/vendors/dec/dec_96.0383

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

As always, Digital urges you to periodically review your system management and security procedures. Digital will continue to review and enhance the security features of its products and work with customers to maintain and improve the security and integrity of their systems.

Hewlett-Packard Company

Included below is information obtained from the February 7th, 1996, Hewlett Packard Security Bulletin, HPSBUX9602-029 "Security Vulnerability in HP-UX *syslog(3)* subroutine."

It has been found that all HP-UX systems prior to HP-UX 10.10 have this vulnerability.

The vulnerability can be eliminated from releases 9.X and 10.0X of HP-UX by applying a patch. Releases of HP-UX prior to 9.X must upgraded to release 9.X or higher to escape the vulnerability, which is fixed in the HP-UX 10.10 release. There are no work-around solutions known.

Hewlett-Packard recommends that all customers concerned with the security of their HP-UX systems either apply the appropriate patch or change perform the actions described above as soon as possible.

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

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

```
                       send guide
```

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

World Wide Web service for downloading of patches is available via our URL:

(http://us.external.hp.com)

```
     Patches:
                 PHCO_6595 (series 700/800, HP-UX 10.0 & 10.01), or
                 PHCO_6598 (series 800, HP-UX 9.0 & 9.04), or
                 PHCO_6597 (series 700, HP-UX 9.0[1357]), or
                 PHCO_6224 (series 300/400, HP-UX 9.0, 9.01, 9.03 & 9.1), or
                 PHCO_6162 (series 700, HP-UX 9.08 BLS), or
                 PHCO_6161 (series 700, HP-UX 9.09 BLS), or
                 PHCO_6160 (series 700, HP-UX 9.09+ BLS), or
                 PHCO_6157 (series 700, HP-UX 10.09 BLS CMW).

     Availability:
             All patches are available now, except for the BLS patches,
             which will be available after 29 February, 1996.  Contact your
             FCO representative for patch availability.
```

Further details are provided in Hewlett-Packard Security Bulletin, "HPSBUX9602-029 Security Vulnerability in HP-UX *syslog(3)* subroutine."

World Wide Web service for browsing of bulletins is available via our URL:

http://us.external.hp.com

Choose "Support news", then under Support news,
Choose "Security Bulletins"

IBM Corporation

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

```
        AIX 4.1 - IX53718
        AIX 3.2 - IX53358
```

Open Software Foundation

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

The Santa Cruz Operation (SCO)

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

ftp://ftp.sco.COM/Supplements/net100/

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

Silicon Graphics Inc.

Silicon Graphics released Security Advisory 19951001-01-P825 and patch 825 to address the specifics of CERT Advisory CA-95.13. Please note that patch 1146 (Security Advisory 19960203-01-P1146) supersedes patch 825. This patch addresses additional security problems in the "sendmail" program. Please refer to SGI Advisory 19960203-01-P1146 for further information on these additional security problems, and the location and checksums of this patch.

Silicon Graphics has continued to investigate the 8lgm reported syslog vulnerability. A review of utilities supplied with the IRIX 5.3, 6.0, 6.0.1 and 6.1 environments that use syslog has been performed. Silicon Graphics has not discovered any syslog vulnerabilities in these utilities.

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

Solbourne (Grumman)

Solbourne 2.5 is not vulnerable.

Sony Corporation

NEWS-OS 6.0.3 and 6.1 are not vulnerable.

Sun Microsystems, Inc.

SunOS 5.5 is not vulnerable.

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

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

Note also that the following patches:

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

require that you contact your Sun Solution Center or other SunSoft authorized service provider (ASP) in the U.S. to obtain a copy of the actual patch.

Sun Security Bulletins are available via the security-alert alias (security-alert@sun.com) and on SunSolve (http://sunsolve1.sun.com).

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

Revision History

```
Sep. 23, 1997  Updated copyright statement
Aug. 30, 1996  Information previously in the README was inserted
               into the advisory.
July 05, 1996  Appendix, Digital- Added pointer to updated information.
July 01, 1996  Appendix, SGI - Added additional information
Apr. 17, 1996  Appendix, SCO - Added an entry for SCO
Mar. 29, 1996  Appendix, Sun - Modified the Sun entry
Feb. 27, 1996  Appendix, Hewlett-Packard & Sun - Updated entries
Feb. 06, 1996  Appendix, Allman & Cray - Updated entries
Dec. 19, 1995  Appendix, Digital -  Modified Digital entry
Nov. 07, 1995  Appendix, IBM, SGI, Sun - Updated entries
Nov. 07, 1995  Sec. III.C - Added note recommending smrsh though it doesn't
               address the particular vulnerability described in the advisory
Oct. 27, 1995  Appendix, Convex, Data General Hewlett-Packard, IBM - Added
               text
```