CERT Advisory CA-1993-16a Sendmail Vulnerability - supplementary advisory containing vendor patch information

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

==========
CERT(sm) Advisory CA-93:16a
Original issue date: January 7, 1994
Last revised: August 30, 1996
Information previously in the README was put into the advisory.
NOTE: SUPERSEDED BY CA-95:05 on February 22, 1995

Topic: Sendmail Vulnerability - supplementary advisory containing vendor patch information
- ----------

*** THIS ADVISORY IS SUPERSEDED BY CA-95:05. ***

The CERT Coordination Center is continuing to work with vendors on eliminating a group of vulnerabilities in sendmail(8). These vulnerabilities include those related to mailing to a program, mailing to a file, and a few others.

This advisory provides information about new patches available from some vendors. At the time that CA-93:16.sendmail.vulnerability was published a set of workarounds were provided. These workarounds should still be used until vendor patches are available. Once the vendor patches have been installed, sites should continue to use smrsh.

CERT/CC has provided detailed information about all known vulnerabilities in sendmail to all of our vendor contacts. If your vendor is unaware of the problems, or if they have any questions, please have them contact us.

Information about available patches as well as information on upcoming patches is provided in Appendix A below.

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

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

.....
Appendix A

The following is vendor-supplied information. Please notice that some entries provide pointers to vendor advisories. For more up-to-date information, contact your vendor.

- ----------
Eric Allman, 8.6.8.1

Version 8.6.8.1 is available for anonymous FTP from ftp.cs.berkeley.edu in the "ucb/sendmail" directory.

Standard Unix Sum
sendmail.8.6.8.base.tar.Z: 05865 486

System V Sum
57100 972 sendmail.8.6.8.base.tar.Z

MD5 Checksum
MD5 (sendmail.8.6.8.base.tar.Z) = 5cacff3e069ae4885402991e1e270386

- ----------

Paul Pomes, IDA:

A new release is available for anonymous FTP from vixen.cso.uiuc.edu
as "pub/sendmail-5.67b+IDA-1.5.tar.gz".

```
                Standard Unix Sum
sendmail-5.67b+IDA-1.5.tar.gz:  17272 1341

                  System V Sum
30425 2682 sendmail-5.67b+IDA-1.5.tar.gz

                  MD5 Checksum
MD5 (sendmail-5.67b+IDA-1.5.tar.gz) = a9b8e17fd6d3e52739d2195cead94300
```

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

BSDI

BSDI can supply either an easy-to-install port of the smrsh patch from
CERT or a port of sendmail-8.6.4 (contact BSDI Customer Support for
information in obtaining either of these solutions). In future
releases, BSDI will ship the newer sendmail that is not affected
by these problems. Releases affected by this advisory: BSD/386 V1.0.

BSDI Contact Information:

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

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

Data General Corporation

Patches are available from dg-rtp.rtp.dg.com (128.222.1.2) in
the directory "deliver/sendmail":

```
Rev             Patch Number            Sys V Checksum
------------    ------------------      --------
5.4.2           tcpip_5.4.2.p14         39298 512
MD5 (tcpip_5.4.2.p14) = c80428e3b791d4e40ebe703ba5bd249c

5.4R2.01        tcpip_5.4R2.01.p12      65430 512
MD5 (tcpip_5.4R2.01.p12) = 9c84cfdb4d79ee22224eeb713a414996

5.4R2.10        tcpip_5.4R2.10.p05      42625 512
MD5 (tcpip_5.4R2.10.p05) = 2d74586ff22e649354cc6a02f390a4be
```

These patches are loadable via the "syadm" utility and installation
instructions are included in the patch notes.

Trusted versions of DG/UX will use the same patches as
their base version of DG/UX.

Customers with any questions about these patches should contact
their local SEs or Sales Representatives.

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

Digital Equipment Corporation

Systems affected: ULTRIX Versions 4.3 (VAX), ULTRIX V4.3 & V4.3A (RISC),
DEC OSF/1 V1.2 & V1.3, using sendmail. The following patches are
available from your normal Digital support channel:

```
ULTRIX V4.3 (VAX), V4.3 (RISC) or V4.3a (RISC):  CSCPAT #: CSCPAT_4044
                            OSF/1  V1.2 and  V1.3:  CSCPAT #: CSCPAT_4045
```

*These fixes will be included in future releases of ULTRIX and DEC OSF/1

Digital Equipment Corporation strongly urges Customers to upgrade
to a minimum of ULTRIX V4.3 or DEC OSF/1 V1.2, then apply the
Security kit to prevent this potential vulnerability.

The full text of Digital's advisory can be found in
/pub/vendors/dec/advisories/sendmail on info.cert.org.

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

Hewlett-Packard Company

For HP/UX, the following patches are available:

PHNE_3369 (series 300/400, HP-UX 8.x), or
PHNE_3370 (series 300/400, HP-UX 9.x), or
PHNE_3371 (series 700/800, HP-UX 8.x), or
PHNE_3372 (series 700/800, HP-UX 9.x), or
modify the sendmail configuration file (releases of HP-UX prior to 8.0)

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

The full text of Hewlett-Packard's advisory can be found in /pub/vendors/hp/advisories/sendmail on info.cert.org.

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

IBM

Patches for these problems can be ordered as APAR# ix40304 and APAR# ix41354. Ix40304 is available now and ix41354 will be sent as soon as it is available.

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

NeXT, Inc.

A patch is available via anonymous FTP from FTP.NEXT.COM in the directory "/pub/NeXTanswers/Files/Patches/SendmailPatch.23950.1".

Filename	Checksum
1513_SendmailPatch.ReadMe.rtf	63963 4
MD5 checksum = 8f561a9bdeb11bc0e0201874dbb7c234	
1514_SendmailPatch.pkg.compressed	02962 290
MD5 checksum = 8c33f32bb4e96f5a9938298ed15ef940	

This patch is also available via electronic mail by sending a message to NeXTanswers@NeXT.com with a subject line of "1513 1514". The two files noted above will be returned as NeXTmail attachments.

This patch is for NEXTSTEP 3.1 and NEXTSTEP 3.2. Instructions for installing this patch are included in the ReadMe file.

Questions about this patch should be directed to NeXT's Technical Support Hotline (1-800-848-NeXT) or via email to ask_next@NeXT.com.

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

The Santa Cruz Operation

Support level Supplement (SLS) net379A, is available for the following platforms:

SCO TCP/IP Release 1.2.0 for SCO UNIX or SCO XENIX
SCO TCP/IP Release 1.2.1 for SCO UNIX
SCO Open Desktop Release 2.0, 3.0
SCO Open Desktop Lite Release 3.0
SCO Open Server Network System, Release 3.0
SCO Open Server Enterprise System, Release 3.0

This SLS is currently available for anonymous ftp download from ftp.sco.COM, (132.147.106.6). The files to download are:

file name	sum -r	
/SLS/net379a.Z	59954 562	<- Supplement file
/SLS/net379a.ltr.Z	19608 6	<- cover letter
/SLS/README	<- general info on how to copy Supplement file to diskette before installing	

	Standard Unix Sum	
/SLS/net379a.Z:	59954	281
/SLS/net379a.ltr.Z:	19608	3

MD5 Checksum
MD5 (/SLS/net379a.Z) = 280c989029f0c8cecefa1f7a397971ff
MD5 (/SLS/net379a.ltr.Z) = 71d764c68263cb4d0b94ccaf1c4818ab

This SLS is also available for UUCP download from the machines

listed below. The file names are:

/usr/spool/uucppublic/SLS/net379a.Z
/usr/spool/uucppublic/SLS/net379a.ltr.Z
/usr/spool/uucppublic/SLS/info (same as README file above)

USA, Canadian, Pacific Rim, Asia, and Latin American customers:

Machine name: sosco
UUCP user: uusls (no password)
Modem Phone numbers:
Telebit Trailblazer Plus 408-429-1786 9600 baud
Telebit 1500 V.32, 2@ 408-425-3502 2400, 9600 baud
Hayes V Series 9600, 2@ 408-427-4470 9600 baud

for Europe, the Middle East, and Africa:

Machine name: scolon
UUCP user: uusls
Password: bbsuucp
Modem Phone numbers:
Dowty Trailblazer +44 (0)923 210911

Hardcopy versions of SLS net379A should also be available from your Support provider, or SCO. If you need to contact SCO to order this SLS, please do so as follows:

Electronic mail: support@sco.COM

The Americas, Pacific Rim, Asia, and Latin America:
6am-5pm Pacific Standard Time (PST)

1-408-425-4726 (voice)
1-408-427-5443 (fax)

Europe, Middle East, Africa: 9am-5:30pm British Standard Time (BST)

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

- ---

Sequent Computer Systems

Versions 3.0.17 and greater of Dynix are vulnerable as are versions 2.2 and 2.3 of the TCP package for PTX.

Sequent customers should call the Sequent Hotline at (800) 854-9969 and ask for the Sendmail Maintenance Release Tape. Alternatively, ptx customers can upgrade to PTX/TCP/IP version 2.2.3 or 2.3.1 as appropriate.

- ---

Silicon Graphics, Inc.

The sendmail vulnerabilities are fixed in IRIX 5.1.1.3 and later systems. Patches for IRIX 4.* and IRIX 5.* systems are available via anonymous FTP from ftp.sgi.com (192.48.153.1) in the directory "sgi/IRIX4.0/sendmail" or "sgi/IRIX5.0/sendmail", respectively. In each directory are four files:

README - describes the other files
sendmail.latest - replacement sendmail binary
sendmail.cf.latest - sample configuration file
sendmail.cf.auto.latest - sample auto configuration file

The sendmail.cf.* files are provided for completeness. Sites should be able to continue to use their locally modified sendmail.cf files.

Customers without Internet access should contact the support center for their country using the procedures outlined in their maintenance agreement for a new sendmail binary.

A. IRIX4.0/sendmail/

Filename	BSD Checksum	SVR4 Checksum
README	10278 2	63012 4

MD5 (IRIX4.0/README) = 13a8ae43cb0d63a165fd48dccf2f45a5

sendmail.cf.auto.latest 35252 34 52100 67

```
      MD5 (IRIX4.0/sendmail.cf.auto.latest) = acec5e81cc6c2119a553dea6bdd9a937

        sendmail.cf.latest      38770 32    20186 6
      MD5 (IRIX4.0/sendmail.cf.latest) = 59a60c6602633688dd4bf6af51d63894

        sendmail.latest         19044 580   50838 1160
      MD5 (IRIX4.0/sendmail.latest) = 358d6930187ba2750e59c66204a9a9c9

        B.  IRIX5.0/sendmail/

        Filename                BSD         SVR4
                                Checksum    Checksum
        ---------------         ---------   ---------

       README                  05005 2         30863 3
       MD5 (IRIX5.0/README) = b5166089628b8da019c04d33141840a3

       sendmail.cf.auto.latest 42039 34        58171 67
       MD5 (IRIX5.0/sendmail.cf.auto.latest) = f11fc9739e67315a218217835bb6328e

       sendmail.cf.latest      47744 32        26263 64
       MD5 (IRIX5.0/sendmail.cf.latest) = 75d09eeffc3980e43c6f3764d227e6d6

       sendmail.latest         47861 918       48212 1836
       MD5 (IRIX5.0/sendmail.latest) = e64fb2296a93d49511c1bb5da994a4fb

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

Solbourne Computer, Inc.

        Patch p93122301 is available from Solbourne to fix the sendmail
        problems.  This patch is equivalent to Sun patch 100377-08.
        Customers may retrieve it via anonymous FTP from
        solbourne.solbourne.com in the pub/support/OS4.1B directory:

        Filename         BSD         SVR4
                         Checksum    Checksum
        ---------------  ---------   ---------
        p93122301.tar.Z  63749 211   53951 421
        MD5 (p93122301.tar.Z) = f7300f3ecfbbbfaa11a6695f42f14615

        It is also available by sending email to solis@solbourne.com
        and specifying "get patches/4.1b p93122301" in the body of the
        mail message.

        Earlier versions (4.1A.*) are no longer supported. The 4.1B
        patch may well work on 4.1A.* systems but this has not been tested.
        If you have any questions please call the SOURCE at 1-800-447-2861 or
        send email to support@solbourne.com.

        The full text of Solbourne's advisory can be found in
        /pub/vendors/solbourne/advisories/sendmail on info.cert.org.

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

Sony Corporation

        These vulnerabilities have been fixed in NEWS-OS 6.0.1.
        A patch is available for NEWS-OS 4.x.  Customers should
        contact their dealers for any additional information.

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

Sun Microsystems, Inc.

        Sun has made patches for sendmail available as described in
        their SUN MICROSYSTEMS SECURITY BULLETIN: #00125, 12/23/93.
        These patches can be found in the
        /systems/sun/sun-dist directory on ftp.uu.net:

        System       Patch ID    Filename        BSD         SVR4
                                                 Checksum    Checksum
        ------       --------    ---------------  ---------   ---------
        SunOS 4.1.x  100377-08  100377-08.tar.Z  05320 755   58761 1510
        Solaris 2.1  100840-06  100840-06.tar.Z  59489 195   61100 390
        Solaris 2.2  101077-06  101077-06.tar.Z  63001 179   28185 358
        Solaris 2.3  101371-03  101371-03.tar.Z  27539 189   51272 377

        MD5 checksums are:
        MD5 (100377-08.tar.Z) = 8e8a14c0a46b6c707d283cacd85da4f1
        MD5 (100840-06.tar.Z) = 7d8d2c7ec983a58b4c6a608bf1ff53ec
        MD5 (101077-06.tar.Z) = 78e165dec0b8260ca6a5d5d9bdc366b8
        MD5 (101371-03.tar.Z) = 687d0f3287197dee35941b9163812b56
```

A patch for x86 based systems will be forthcoming as patch 101352-02.

4.1 sites installing these patches may require sites to modify
their configuration files slightly. Full details are given in
the Sun advisory.

The full text of Sun Microsystems's advisory can be found in
/pub/vendors/sun/advisories/sendmail on info.cert.org.

- --
The CERT Coordination Center wishes to thank all the vendors for
recognizing the importance of these vulnerabilities and responding
to them.
- --

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

Internet E-mail: cert@cert.org
Telephone: 412-268-7090 (24-hour hotline)
           CERT personnel answer 8:30 a.m.-5:00 p.m. EST(GMT-5)/EDT(GMT-4),
           and are on call for emergencies during other hours.

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890

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

~~~~~~
Revision history

Aug. 30, 1996 Information previously in the README was inserted
               into the advisory. A summary list of vendor names was
               removed from the body of the advisory.
July 25, 1996 Introduction - changed statement about using smrsh to say that
               sites should continue to use it after installing vendor patches.
Feb. 22, 1995 This advisory was further superseded by CA-95:05.
July 14, 1994 This advisory was superseded by CA-94:12.
Nov. 07, 1994 Immediately before the appendix - added a note about smrsh.
  --   Appendix - updated vendor information as it was received.

-----BEGIN PGP SIGNATURE-----
Version: PGP for Personal Privacy 5.0
Charset: noconv

iQA/AwUBOBS961r9kb5qlZHQEQIGdgCdGMTGoaqfytguYoD7djb9wFBNvmEAoL9q
OsJdXMrUx6oEvSVAmJgMvdOR
=o62B
-----END PGP SIGNATURE-----
~~~~~~