CERT Advisory CA-1994-12 Sendmail Vulnerabilities

==
CERT (sm) Advisory CA-94:12
Original issue date: July 14, 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              Note: SUPERSEDED BY CA-95:05 on February 22, 1995.

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

Topic: Sendmail Vulnerabilities

- ---

         *** THIS ADVISORY HAS BEEN SUPERSEDED BY CA-95:05. ***

There are two vulnerabilities in some vendors' versions of sendmail(8).
One, in the debug option, enables local users to gain root access. The other,
in the error message header option, enables local users to read any file on
the system. Both vulnerabilities are known in the intruder community.

The CERT Coordination Center is in contact with vendors concerning these
vulnerabilities. Those who have patches available are listed at the end of
this advisory. If your vendor's name is not on the list, contact the vendor
directly for information on whether their version of sendmail(8) is vulnerable
and, if so, whether a patch is 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

There is a problem with the debug option (-d) and/or the error message header
option (-oE) in some vendors' versions of sendmail(8). An exploitation
script has been circulated for sendmail -d, and intruders are actively
exploiting this vulnerability. As of the date of this advisory, we have not
received reports of the sendmail -oE vulnerability being exploited.

II. Impact

     The sendmail -d vulnerability allows local users to gain root access.
     The sendmail -oE vulnerability allows local users to read any file on
     the system.

III. Solution

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

     Below is a summary of the vendors listed in Appendix A.
     We will update the appendix as we receive more information from vendors.

     Vendor or Source

     Eric Allman
     Amdahl
     Apple
     Berkeley Software Design
     Berkeley Software Distribution
     Convex
     Data General
     Digital Equipment
     Hewlett Packard
     IBM
     IDA
     Open Software Foundation
     Santa Cruz Operation
     Sun

     Note: Some sites may find it feasible to install Eric Allman's
     sendmail, which is freely available (see the appendix for
     details). However, depending upon the currently installed sendmail
     program, switching to a different sendmail may require significant
     effort. The site administrator may need to become familiar with the
     new program, and the site's sendmail configuration file may require
     considerable modification in order to provide existing functionality.

....
Appendix: Vendor Information

Below is information we have received from vendors who have patches available
or upcoming for the vulnerabilities described in this advisory, as well as
vendors who have confirmed that their products are not vulnerable. If your
vendor's name is not in one of these lists, contact the vendor directly for
information on whether their version of sendmail is vulnerable and, if so, the
status of patches to address the vulnerabilities.

- ---------------------------------------
Eric Allman

Sendmail versions 8.6.8 and 8.6.9 are not vulnerable. The problem with -d was
fixed in sendmail 8.6.7, and -oE was fixed in sendmail 8.6.8. Even if you are
running 8.6.8, you may want to upgrade to 8.6.9 for the additional features.

Version 8.6.9 is available by anonymous FTP from ftp.cs.berkeley.edu in the
directory ucb/sendmail.

        MD5 (sendmail.8.6.9.base.tar.Z) = 9bffb19116e7fdbb6ec56ccf9344895b
        MD5 (sendmail.8.6.9.cf.tar.Z) = 37ecb776ec61f596d01fbb46bae6e72f
        MD5 (sendmail.8.6.9.misc.tar.Z) = e083dbd609bdaf4b46c52f2546b3d1e5
        MD5 (sendmail.8.6.9.xdoc.tar.Z) = 0df46586fbe767bf7060068331de7186

- ---------------------------------------
Amdahl

All versions of UTS 2.1 use smail rather than sendmail and are not vulnerable
to these problems.

- ---------------------------------------
Apple Computer, Inc.

A patch to version 3.1 of A/UX for these vulnerabilities is available by
anonymous FTP from ftp.support.apple.com or aux.support.apple.com; in each
case, a compressed, replacement version (8.6.4.1) of sendmail is in
pub/aux.patches.

```
Filename        sendmail.Z
BSD checksum    02992  182
SysV checksum   10129  364
MD5 checksum    df4ca82f624ee8f4404c5e979e7e3d24
```

Uncompress this file using compress(1) and replace the previous version
(8.6.4) in /usr/lib; be sure to kill the running sendmail and restart.

Earlier versions of A/UX are not supported by this patch. Users of previous
versions are encouraged by Apple to update their system to A/UX 3.1 or compile
and install the version of sendmail available from ftp.cs.berkeley.edu.

Customers should contact their reseller for any additional information.

- ---------------------------------------
Berkeley Software Design (BSDI)

Patches to sendmail for these problems in BSD/386 V1.1 are available from BSDI
customer support:

```
                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
```

- ---------------------------------------
Berkeley Software Distribution (BSD)

4.4BSD-Lite uses sendmail version 8.6.9 and thus is not vulnerable.

- ---------------------------------------
Convex

ConvexOS 11.0 (the most recent production OS) does not contain the
vulnerabilities.

Convex customers running ConvexOS 10.x should install the CONVEX TAC PATCH
10.3.129, which is the full ConvexOS 11.0 mail system back ported to ConvexOS

10.x.

The 10.3.129 README file is reproduced below:
The following patch information is provided by a member of the
CONVEX TAC. There is no express or implied warranty. The maintenance
of this patch is the responsibility of the installer. The existence of
this patch does not guarantee that the patch or its functionality
will be available in the next release of the product.

PATCH PRODUCT NAME: ConvexOS Mail System
PATCH FOR VERSION NUMBER: 10.3
PATCH MODULE NAME: /usr/lib/sendmail
NEW VERSION NUMBER OF PRODUCT: 10.3.129
RELATED BUG REPORTS: X-33414, X-33531

PATCH INSTALLATION:
 Pre-installation precautions:

 if from tape:
        %tpmount
        %installsw -i

        NOTE: If installing from tape, you must use a no-rewind tape
        device, such as /dev/rmt20 or /dev/rdat0n, /dev/eb0nr, or
        /dev/rtc0n.

 if from script:
        % ./Script.sh

The Convex Technical Assistance Center is available for additional
information at 800-952-0379.

- --
Data General Corporation

DG/UX systems are not at risk from the -oE problem.

Patches will be made available for all supported releases of DG/UX for the -d
problem and it will be fixed in future releases of DG/UX starting with DG/UX
5.4 Release 3.10. Affected sites should call their Customer Support Center
for information regarding this patch.

- --
Digital Equipment Corporation

[The following information was excerpted from DEC SECURITY ADVISORY #0505 and
information about DEC OSF/1 was updated by Digital on Feb. 1, 1995.]

Products Affected:
        ULTRIX   Versions 4.3, 4.3A, V4.4
        DECnet-ULTRIX Version 4.2
        DEC OSF/1   Versions 1.2, 1.3, 1.3A, 2.0

SOLUTION: ULTRIX: Upgrade/Install ULTRIX to an minimum of V4.4 and install the
          Security Enhanced Kit

           DEC OSF/1, upgrade/install to a minimum of V2.0 (not V1.2)
           before installing the Security Enhanced Kit.

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

These kits are available from Digital Equipment Corporation by contacting
your normal Digital support channel or by request via DSNlink for electronic
transfer.

KIT PART NUMBERS and DESCRIPTIONS

CSCPAT_4060 V1.0   ULTRIX   V4.3 thru V4.4 (Includes DECnet-ULTRIX V4.2)
CSCPAT_4061 V1.0   DEC OSF/1 V1.2 thru V2.0

         These kits will not install on versions previous to ULTRIX V4.3
         or DEC OSF/1 V1.2.

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.

    NOTE: For non-contract/non-warranty customers contact your local Digital
          support channels for information regarding these kits.

- --
Hewlett-Packard

HP/UX does not support the -oE option.

To fix the -d problem, obtain patch PHNE_4533 from Hewlett-Packard. This patch 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 by anonymous FTP from info.cert.org in the file "pub/vendors/hp/supportline_and_patch_retrieval".

- --
IBM

A patch for the -d vulnerability can be ordered from IBM as APAR IX44020 (PTF U431041). AIX is not vulnerable to the -oE problem. To order APARs from IBM in the U.S., call 1-800-237-5511 and ask that it be shipped to you as soon as it is available. To obtain APARs outside of the U.S., contact your local IBM representative.

- --
IDA, Paul Pomes

The current version "sendmail-5.67b+IDA 1.5" is not vulnerable.

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

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

- --
Open Software Foundation (OSF)

For OSF/1 R1.3:
CR11057 describes how to fix the -d option problem in the sources.
OSF/1 is not vulnerable to the -oE problem.

- --
The Santa Cruz Operation, Inc. (SCO)

SCO systems are not affected by the -oE problem and a patch for the -d problem on the following platforms will soon be available:

SCO TCP/IP Release 1.2.0 for SCO XENIX
SCO TCP/IP Release 1.2.1 for SCO UNIX
SCO Open Desktop Release 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

For more information contact SCO at:

Electronic mail: support@sco.COM

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

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

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

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

- --
Sun Microsystems, Inc.

A. Patch list

Sun has produced patches against these vulnerabilities for the versions of SunOS shown below.

4.1.1	100377-15	
4.1.2	100377-15	
4.1.3	100377-15	
4.1.3_U1	101665-02	
5.1_x86	101352-03	(Solaris x86)
5.1	100834-11	(Solaris 2.1)
5.2	100999-59	(Solaris 2.2)

5.3	101318-41	(Solaris 2.3)

B. Patch notes

1. The last security-related patch for 4.1.x sendmail was distributed as 100377-08 (announced 23 December 1993). Revisions -09 through -14 were not related to security.

2. The 4.1.1 patch includes a version built for the sun3 architecture.

3. The 4.1.3 version of the patch is also applicable to 4.1.3C systems.

4. The patch listed for 4.1.3_U1 (Solaris 1.1.1) applies to both the A and B versions. This is currently true for all U1 patches.

5. One of the listed patches (100834-11, for SunOS 5.1) is actually a jumbo kernel patch into which sendmail was bundled. The other two SunOS 5.x patches, and all of the 4.1.x patches, contain only sendmail fixes. (Sun bundled all 5.x sendmails into jumbo kernel patches earlier this year, but later unbundled the 5.3 and 5.2 patches in response to customer complaints. The 5.1 sendmail will be unbundled as well later this summer.

6. Sun releases new patch versions frequently. For this reason, when requesting patches you should ask for the specified "or later" version, e.g., "version 11 or later of patch 100834".

Patches can be obtained from local Sun Answer Centers and Sunsolve. U.S. users can contact Sun a 800-USA-4SUN. Sun can also be reached by e-mail at security-alert@sun.com.

- ----------

- ----------

The CERT Coordination Center wishes to thank all the vendors listed in this advisory for their efforts in responding to this problem.

- ----------

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).

If you wish to send sensitive incident or vulnerability information to CERT via electronic mail, CERT strongly advises that the e-mail be encrypted. CERT can support a shared DES key, PGP (public key available via anonymous FTP on info.cert.org), or PEM (contact CERT for details).

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
USA

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 and the vendor list in Sec. III abbreviated.
Feb. 22, 1995	Superseded by CA-95:05.
Feb. 2, 1995	Appendix, Digital - modified information from Digital.

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

iQA/AwUBOBS9+Vr9kb5qlZHQEQKjtQCgtfDUKlhKfftMdZohdXlOm1JwSPsAoMiT
~~~~~~

OMu7PFEfbneB2wr1nDsRUz+Y
=LRSL
-----END PGP SIGNATURE-----