CERT Advisory CA-1996-24 Sendmail Daemon Mode Vulnerability

Original issue date: November 21, 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 serious security problem in sendmail that affects versions 8.7 through 8.8.2. By exploiting this vulnerability, any local user can gain root access. Exploitation details involving this vulnerability have been widely distributed.

Independent of this new vulnerability, there are other security problems with older sendmail versions. Even if you are not running a version between 8.7 and 8.8.2, we strongly encourage you to upgrade to the current version of sendmail (8.8.3). See Section IV for details.

The CERT/CC team recommends installing vendor patches or upgrading to the current version of sendmail (8.8.3). Until you can do so, we urge you to apply the workaround provided in Section III.C. In all cases, be sure to take the extra precautions listed in Section III.D.

We will update this advisory as we receive additional information. Please check advisory files regularly for updates that relate to your site. In addition, you can check ftp://ftp.cert.org/pub/latest_sw_versions/sendmail to identify the most current version of sendmail.

I. Description

Sendmail is often run in daemon mode so that it can "listen" for incoming mail connections on the standard SMTP networking port, usually port 25. The root user is the only user allowed to start sendmail this way, and sendmail contains code intended to enforce this restriction.

Unfortunately, due to a coding error, sendmail can be invoked in daemon mode in a way that bypasses the built-in check. When the check is bypassed, any local user is able to start sendmail in daemon mode. In addition, as of version 8.7, sendmail will restart itself when it receives a SIGHUP signal. It does this restarting operation by re-executing itself using the *exec(2)* system call. Re-executing is done as the root user. By manipulating the sendmail environment, the user can then have sendmail execute an arbitrary program with root privileges.

II. Impact

Local users can gain root privileges on the local machine.

III. Solution

Install a patch from your vendor if one is available (Section A) or upgrade to the current version of sendmail (Section B). Until you can take one of those actions, we recommend applying the workaround described in Section C. In all cases, you should take the precautions described in Section D.

A. Install a vendor patch.

Below is a list of vendors who have provided information about sendmail. Details are in Appendix A of this advisory; we will update the appendix as we receive more information. If your vendor's name is not on this list, please contact the vendor directly.

Berkeley Software Design, Inc. (BSDI)
Data General Corporation
Digital Equipment Corporation
FreeBSD
Hewlett-Packard Company
IBM Corporation
Linux
NeXT Software, Inc.
Open Software Foundation (OSF)
The Santa Cruz Operation, Inc. (SCO)
Silicon Graphics, Inc.
Sun Microsystems, Inc.

B. Upgrade to the current version of sendmail.

Install sendmail 8.8.3. This version is a "drop in" replacement for 8.8.x. There is no patch for any version of sendmail before 8.8.0. If you are running such a version, strongly consider moving to version 8.8.3.

Sendmail 8.8.3 is available from

ftp://ftp.sendmail.org/ucb/src/sendmail/sendmail.8.8.3.tar.gz

ftp://ftp.cert.org/pub/tools/sendmail/sendmail.8.8.3.tar.gz

ftp://ftp.cert.dfn.de/pub/tools/net/sendmail/sendmail.8.8.3.tar.gz

ftp://ftp.auscert.org.au/pub/mirrors/ftp.cs.berkeley.edu/ucb/sendmail/*

MD5 (sendmail.8.8.3.tar.gz) = 0cb58caae93a19ac69ddd40660e01646

Also in that directory are .Z and .sig files. The .Z file contains the same bits as the .gz file, but is compressed using UNIX compress instead of gzip. The .sig is Eric Allman's PGP signature for the uncompressed tar file. The key fingerprint is

```
Type bits/keyID    Date       User ID
  pub  1024/BF7BA421 1995/02/23 Eric P. Allman <eric@CS.Berkeley.EDU>
            Key fingerprint =  C0 28 E6 7B 13 5B 29 02  6F 7E 43 3A 48 4F 45 29
                               Eric P. Allman <eric@Reference.COM>
                               Eric P. Allman <eric@Usenix.ORG>
                               Eric P. Allman <eric@Sendmail.ORG>
                               Eric P. Allman <eric@CS.Berkeley.EDU>
```

When you change to a new version of sendmail, we strongly recommend also changing to the configuration files that are provided with that version. Significant work has been done to make this task easier. (In fact, it is highly likely that older configuration files will not work correctly with sendmail version 8.) It is now possible to build a sendmail configuration file (sendmail.cf) using the configuration files provided with the sendmail release. Consult the cf/README file for a more complete explanation. Creating your configuration files using this method makes it easier to incorporate future changes to sendmail into your configuration files.

Sun sendmail users: A paper is available to help you convert your sendmail configuration files from the Sun version of sendmail to one that works with sendmail version 8.8.x. 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.

C. Apply a workaround.

Eric Allman, the author of sendmail, has provided the following workaround.

This vulnerability relies on a coding error that has existed in sendmail since November 1982, allowing non-root users to start up an SMTP daemon by invoking sendmail as smtpd. However, that error did not have the current negative implications until sendmail added the ability to re-execute when a SIGHUP signal was received; this was added in 8.7.

The anti-smtpd program given in Appendix B refuses to permit sendmail to be invoked as smtpd by a non-root user. It should be installed setuid root in place of sendmail (e.g., as /usr/sbin/sendmail or /usr/lib/sendmail, depending on your system); the real sendmail should be moved to another place. That location should be set in the REAL_SENDMAIL definition, and it should not be accessible by ordinary users. This permits the anti-smtpd program to moderate access to sendmail.

D. Take additional precautions

Regardless of which solution you apply, you should take these extra precautions to protect your systems. These precautions do not address the vulnerabilities described herein, but are recommended as good practices to follow for the safer operation of sendmail.

- Use the sendmail restricted shell program (smrsh)

With *all* versions of sendmail, use the sendmail restricted shell program (smrsh). You should do this whether you use vendor-supplied sendmail or install sendmail yourself. Using smrsh gives you improved administrative control over the programs sendmail executes on behalf of users.

A number of sites have reported some confusion about the need to continue using the sendmail restricted shell program (smrsh) when they install a vendor patch or upgrade to a new version of sendmail. You should always use the smrsh program.

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

smrsh is also distributed with some operating systems.

- Use mail.local

If you run /bin/mail based on BSD 4.3 UNIX, replace /bin/mail with mail.local, which is included in the sendmail distribution. As of Solaris 2.5 and beyond, mail.local is included with the standard distribution. It is also included with some other operating systems distributions, such as FreeBSD.

Although the current version of mail.local is not a perfect solution, it is important to use it because it addresses vulnerabilities that are being exploited. For more details, see CERT advisory CA-95.02.

To use mail.local, replace all references to /bin/mail with /usr/lib/mail.local. If you are using the M4(1)-based configuration scheme provided with sendmail 8.X, add the following to your configuration file:

define(`LOCAL_MAILER_PATH', /usr/lib/mail.local)

- WARNING: Check for setuid executable copies of old versions of mail programs

If you leave setuid executable copies of older versions of sendmail installed in /usr/lib (on some systems, it may be installed elsewhere), the vulnerabilities in those versions could be exploited if an intruder gains access to your system. This applies to sendmail.mx as well as other sendmail programs. Either delete these versions or change the protections on them to be non-executable.

Similarly, if you replace /bin/mail with mail.local, remember to remove old copies of /bin/mail or make them non-executable.

IV. Additional Notes

Two other sendmail vulnerabilities are described in CERT advisory CA-96.20; see that advisory for details.

Since the release of CA-96.20, two additional sendmail vulnerabilities have been discovered and fixed. By upgrading to sendmail version 8.8.3, the two problems, noted below, are also fixed. Note that the wrapper described in Section III.C does not address these vulnerabilities. The best advice is to upgrade to sendmail version 8.8.3.

A. A vulnerability in sendmail Versions 8.8.0 and 8.8.1 has been discovered that allows remote users to execute arbitrary commands with root privileges.

This vulnerability exploits exploiting a problem related to a buffer overflow when converting between 7-bit and 8-bit MIME messages. Versions prior to Version 8.8.0 do not contain this vulnerability. Versions before 8.7.6 contain other unrelated vulnerabilities. This vulnerability is fixed in version 8.8.2 and beyond. The Australian Emergency Response Team (AUSCERT) issued an advisory on this vulnerability, AA-96.06a, available from

http://www.auscert.org.au/

ftp://ftp.auscert.org.au/pub/

B. A problem in sendmail has been reported that permits users on a system to redirect any email in the queue addressed to an unqualified domain name to a host of their choosing

that is, they can steal queued email. In some versions of the resolver, they may also be able to steal queued email addressed to fully qualified addresses. This bug is believed to exist in all versions of sendmail up to and including 8.8.0. It is fixed in version 8.8.1 and beyond.

Appendix A - Vendor Information

Below is a list of the vendors who have provided information for this advisory. We will update this appendix as we receive additional information. If you do not see your vendor's name, please contact the vendor directly.

Berkeley Software Design, Inc. (BSDI)

BSD/OS is vulnerable to the sendmail daemon problem and we have issued an official patch (U210-029) which may be obtained from our mail-back patches server at

patches@BSDI.COM

or via anonymous ftp from:

ftp://ftp.bsdi.com/bsdi/patches/patches-2.1/U210-029

Data General Corporation

The sendmail included with Data General's DG/UX is not subject to this vulnerability.

Digital Equipment Corporation

DIGITAL Engineering is aware of these reported problems and testing is currently underway to determine the impact against all currently supported releases of DIGITAL UNIX and ULTRIX. Patches will be developed (as necessary) and made available via your normal DIGITAL Support channel. Notice will be through normal AES services and DIGITAL'S Web site

http://www.service.digital.com/html/whats-new.html

FreeBSD

All currently shipping releases of FreeBSD are affected, including the just released 2.1.6. An update for 2.1.6 will be available shortly. This problem has been corrected in the -current sources. In the mean time, FreeBSD users should follow the instructions in the CERT advisory. Sendmail will compile and operate "out of the box" on FreeBSD systems.

Hewlett-Packard Company

HPSBUX9704-059

HEWLETT-PACKARD SECURITY BULLETIN: #00059, 30 April 1997

Description: Sendmail patches for HP-UX releases 9.X thru 10.20

Security Bulletins are available from the HP Electronic
Support Center via electronic mail.

User your browser to get to the HP Electronic Support
Center page at:

http://us-support.external.hp.com
(for US, Canada, Asia-Pacific, & Latin-America)

http://europe-support.external.hp.com
(for Europe)

IBM Corporation

See the appropriate release below to determine your action.

AIX 3.2
No fix required. AIX 3.2 sendmail is not vulnerable.

AIX 4.1
No fix required. AIX 4.1 sendmail is not vulnerable.

AIX 4.2
AIX 4.2 sendmail is vulnerable.

APAR IX63068 will be available shortly.

To determine if you have this APAR on your system, run the following command:

```
instfix -ik IX63068
```

To Order
APARs may be ordered using Electronic Fix Distribution (via FixDist) or from the IBM Support Center. For more information on FixDist, reference URL:

http://service.software.ibm.com/aixsupport/

or send e-mail to aixserv@austin.ibm.com with a subject of "FixDist".

IBM and AIX are registered trademarks of International Business Machines Corporation.

Linux
Linux has provided these URLs for S.u.S.E. Linux:

ftp://ftp.suse.de/suse_update/S.u.S.E.-4.3/sendmail

ftp://ftp.gwdg.de/pub/linux/suse/suse_update/S.u.S.E.-4.3/sendmail

Checksums for the files in these directories:

```
6279df0597c972bff65623da5898d5dc  sendmail.tgz
0c0d20eecb1019ab4e629b103cac485c  sendmail-8.8.3.dif
0cb58caae93a19ac69ddd40660e01646  sendmail-8.8.3.tar.gz
```

Caldera OpenLinux has released a security advisory, available from

http://www.caldera.com/tech-ref/cnd-1.0/security/SA-96.06.html

Red Hat has patched sendmail 8.7.6.
The fixes are available from

Red Hat Linux/Intel:
rpm -Uvh ftp://ftp.redhat.com/updates/4.0/i386/sendmail-8.7.6-5.i386.rpm

Red Hat Linux/Alpha:
rpm -Uvh ftp://ftp.redhat.com/updates/4.0/axp/sendmail-8.7.6-5.axp.rpm

NeXT Software, Inc.
NeXT is not vulnerable to the problem described in Section IV.A. NeXT is vulnerable to the problem described in Section IV.B, and it will be fixed in release 4.2 of OpenStep/Mach.

Open Software Foundation (OSF)
OSF/1 R1.3 is not vulnerable to this problem.

The Santa Cruz Operation, Inc. (SCO)
SCO is investigating the problem and will have more information in the near future.

If we find that patches are needed, please check the following URLs and this advisory appendix.

ftp://ftp.sco.com/SLS/README

ftp://ftp.sco.com/SSE/README

Silicon Graphics, Inc.
Silicon Graphics has historically provided a version 8.6.x sendmail program. The most recent SGI sendmail patch (1502) provides a version 8.6.12 sendmail program also.

The versions of sendmail provided in the distributed Silicon Graphics IRIX operating system versions 5.2, 5.3, 6.0, 6.0.1, 6.1, 6.2 and 6.3 (and in SGI patch 1502, which is the latest released patch for sendmail) are not vulnerable to the exploitation as described in the CERT Advisory CA-96.24.

No further action is required.

Silicon Graphics also published an advisory for their customers on November 21, 1996--SGI advisory number 19961103-01-I. SGI advisories are available from

http://www.sgi.com/Support/Secur/advisories.html

ftp://sgigate.sgi.com/security/

Sun Microsystems, Inc.

No Sun versions of sendmail are affected by this vulnerability.

Appendix B - anti-smtpd.c

Below is the code for the anti-smtpd.c sendmail wrapper. Here is an example of how to compile and install this wrapper. You may have to change these commands for your system. Further, you may have to change the code for anti-smtpd.c to get it to compile on your system. Finally, you may also have to turn off sendmail before running these commands and then turn sendmail back on after running them. Run these commands as root.

```
# mkdir /usr/hidden
# chmod 700 /usr/hidden
# mv /usr/lib/sendmail /usr/hidden/sendmail
# cc anti-smtpd.c -o anti-smtpd
# mv anti-smtpd /usr/lib/sendmail
# chmod u+s /usr/lib/sendmail
```

Here is the code for anti-smtpd.c:

```
#include <stdio.h>
#include <string.h>
#include <syslog.h>
#include <sysexits.h>
```

```
static char *Version = "Version 1.0 November 21, 1996";


/*
**  Sendmail wrapper for CA-96.24 HUP to smtpd problem
**
**      This is trivial -- it just ensures that sendmail cannot be
**      invoked as smtpd.
**
**      To install this, move the real sendmail into /usr/hidden,
**      which should be a mode 700 directory owned by root. Install
**      this program setuid root in place of sendmail.
*/

#ifndef REAL_SENDMAIL
# define REAL_SENDMAIL  "/usr/hidden/sendmail"
#endif

main(argc, argv)
        int argc;
        char **argv;
{
        char *p;
        extern int errno;

        if (argc < 1)
        {
                fprintf(stderr, "sendmail: need a program name\n");
                exit(EX_USAGE);
        }

        p = strrchr(argv[0], '/');
        if (p == NULL)
                p = argv[0];
        else
                p++;
        if (strcmp(p, "smtpd") == 0 && getuid() != 0)
        {
                fprintf(stderr, "sendmail: cannot be invoked as smtpd\n");
                syslog(LOG_ALERT, "sendmail: invoked as smtpd by %d", getuid());
                exit(EX_USAGE);
        }
        execv(REAL_SENDMAIL, argv);
        fprintf(stderr, "sendmail: cannot exec %s: errno = %d\n",
                REAL_SENDMAIL, errno);
        exit(EX_OSFILE);
}
```

The CERT Coordination Center thanks Eric Allman and AUSCERT for their contributions to the development of this advisory.

Revision History

```
Sep.24, 1997   Updated copyright statement

May 8, 1997    Appendix A - updated vendor information for Hewlett-Packard.
Nov. 22, 1996  Updates - added vendor information for Silicon Graphics.
               Modified Hewlett Packard's patch information.
```