CERT Advisory CA-1996-25 Sendmail Group Permissions Vulnerability

Original issue date: December 10, 1996
Last revised: October 20, 1997
Updated vendor information for Sun.

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

The CERT Coordination Center has received reports of a security problem in sendmail affecting version 8. By exploiting this vulnerability, a local user can run programs with group permissions of other users. For the exploitation to be successful, group-writable files must be available on the same file system as a file that the attacker can convince sendmail to trust.

The CERT/CC team recommends installing vendor patches or upgrading to the current version of sendmail (8.8.4). 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

When sendmail causes mail to be delivered to a program listed in a .forward or :include: file, that program is run with the group permissions possessed by the user who owns that .forward or :include: file. The file's owner attribute is used to initialize the list of group permissions that are in force when the program is run. This list is determined by scanning the /etc/group file, NIS or NIS+ group maps, or other similar vendor-specific databases (such as netinfo on OpenStep).

It is possible for users to obtain group permissions they should not have by linking to a file that is owned by someone else, but on which they have group write permissions. By changing that file, users can acquire the group permissions of the owner of that file.

Exploitation is possible if the attacked user has a file that is group writable by the attacker on the same file system as either (a) the attacker's home directory or (b) an :include: file that is referenced directly from the aliases file and is in a directory writable by the attacker. The first (.forward) attack only works against root. This attack does not give users root "owner" permissions, but does give them access to the groups that list root in /etc/group.

II. Impact

A local attacker can gain the group permissions of another user.

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)
Cray Research
Digital Equipment Corporation
FreeBSD, Inc.
Hewlett-Packard Company
IBM Corporation
NEC Corporation
The Santa Cruz Operation, Inc. (SCO)
Silicon Graphics Inc
Solbourne (Grumman Support Systems)
Sun Microsystems, Inc.

B. Upgrade to the current version of sendmail.

Install sendmail 8.8.4. 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 8.8.4.

Sendmail 8.8.4 is available from

ftp://ftp.sendmail.org/ucb/src/sendmail/sendmail.8.8.4.tar.gz

ftp://ftp.cert.org/pub/tools/sendmail/sendmail.8.8.4.tar.gz

ftp://ftp.cert.dfn.de/pub/tools/net/sendmail/sendmail.8.8.4.tar.gz

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

MD5 (sendmail.8.8.4.tar.gz) = 64ce6393a6968a0dc7c6652dace127b0

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. Note that this workaround is for sendmail 8.8.3. If you are running a version less than 8.8.3 we strongly recommend to upgrade at least to that version (or install the appropriate vendor patches). See CERT advisories CA-95.08 and CA-96.24 for more information on vulnerabilities in older sendmail versions.

Set the UnsafeGroupWrites option in the sendmail.cf file. This option tells sendmail that group-writable files should not be considered safe for mailing to programs or files, causing sendmail to refuse to run any programs referenced from group-writable files. Setting this option is a good idea in any case, but may require your users to tighten permissions on their .forward files and :include: files.

The command "find <filesystem> -user root -type f -perm -020 -print" will print the names of all files owned by root that are group writable on a given file system. While this is only a partial solution we encourage you to carefully check all entries in your alias and .forward files (incl. aliases obtained via NIS, NIS+, or similar information systems) to check for group writable files.

In addition, group memberships should be audited regularly. Users should not be in groups without a specific need. In particular, root generally does not need to be listed in most groups.

As a policy matter, root should have a umask of 022 so that group-writable files are made consciously. Also, the aliases file should not reference :include: files in writable directories.
While checking for writable directories, it's not enough to check the permissions of the directory the file itself lives in. You also have to check all other directories "on top" of that dir. If you, for example, want to check the permissions of the file
/where/ever/here/file you have to check for group-write permissions not only in the directory /where/ever/here but also check the directories /where/ever and /where.

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 Version 8 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

Three other sendmail vulnerabilities are described in CERT advisory CA-96.20 and CA-96.24; see those advisories for details.

Sendmail 8.8.4 also fixes a denial-of-service attack. If your system relies on the TryNullMXList option to forward mail to third-party MX hosts, an attacker can force that option off, thereby causing mail to bounce. As a workaround, you can use the mailertable feature to deliver to third party MX hosts regardless of the setting of the TryNullMXList option.

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.

BSD/OS is vulnerable to this problem and a patch (U210-030) is available from our mail-back patches server at

patches@BSDI.COM

or via ftp at

ftp://ftp.BSDI.COM/bsdi/patches/patches-2.1/U210-030

Cray Research

Sendmail version 8 has not been included in any released Unicos system, so this is not a problem for current Unicos systems.

Digital Equipment Corporation

This problem is currently under review by engineering to determine if it impacts DIGITAL UNIX and DIGITAL ULTRIX sendmail implementations.

FreeBSD, Inc.

FreeBSD versions 2.1.5, 2.1.6, and 2.1.6.1 are affected by the group vulnerability. Versions 2.1.6 and 2.1.6.1 are affected by the denial of service vulnerability. All known sendmail security problems will have been addressed prior to the upcoming 2.2 release. Given the complex nature of the patches produced by the sendmail author, user's are encouraged to follow the workarounds described in this advisory or apply and install patches available directly from the author to upgrade to Sendmail 8.8.4 available from the URLs listed in this advisory.

We believe FreeBSD version 2.1.0 and prior to be unaffected by these particular vulnerabilities, however there are significant other security vulnerabilities in the sendmail supplied in prior releases. All FreeBSD users should consider upgrading to sendmail 8.8.4 or removing sendmail from their systems if they are concerned about unauthorized root access from an unprivileged user account.

Hewlett-Packard Company

Vulnerabilities

1. Sendmail Group Permissions Vulnerability
2. Denial of Service Attack using the sendmail configuration variable TryNullM\XList.

Vulnerable releases

9.x
pre-10.2 10.x
10.2

The 9.x, pre-10.2 10.x sendmail is vulnerable with respect to the "Sendmail Group Permissions Vulnerability".

The 10.2 sendmail is vulnerable with respect to both the reported security holes.

Patches for these vulnerabilities are in progress.

IBM Corporation

The version of sendmail that ships with AIX is vulnerable to the conditions listed in this advisory. A fix is in progress and the APAR numbers will be available soon.

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

NEC Corporation

Checking out the vulnerability. Contacts for further information by e-mail:UX48-security-support@nec.co.jp .

The Santa Cruz Operation, Inc. (SCO)

Any SCO operating system running a version of sendmail provided by SCO is vulnerable to this problem. SCO will soon be providing a Support Level Supplement, (SLS), to address this issue for the following releases of SCO software:

SCO Internet FastStart release 1.0.0, 1.1.0
SCO OpenServer releases 5.0.0 and 5.0.2

The SLS will provide a version of sendmail release 8.8.4 for these platforms.

Note that only SCO Internet FastStart uses sendmail as the default mail system. All other SCO operating systems use other mail systems such as the Multi-Channel Memorandum Distribution Facility (MMDF) or the "mailsurr" mail system as the default, and as such are not vulnerable to this problem unless otherwise configured to use sendmail.

Please watch the following URLs for availability information:

ftp://ftp.sco.COM/SLS/README

ftp://ftp.sco.COM/SSE/README

Silicon Graphics Inc.

Currently Silicon Graphics Inc does not provide a 8.8.x sendmail version but instead provides a 8.6.12 version. Silicon Graphics has evaluated this issue as possibly applicable to the 8.6.12 version provided by Silicon Graphics and has not found this version to be vulnerable. No further action is required.

Solbourne (Grumman Support Systems)

Solbourne customers running the supported sendmail version

SendMail version 1.1 of 92/11/12 are not vulnerable to this 'denial-of-service' attack.

Those Solbourne customers running later versions of sendmail are probably vulnerable and should consider applying the workaround or installing the latest version of sendmail.

No patches are available.

Sun Microsystems, Inc.

Sun Microsystems has provided the following list of patches in response to this advisory:

```
        103594-10 5.5.1
        103595-10 5.5.1_86
        102980-13 5.5
        102981-13 5.5_x86
        102066-18 5.4
        102064-17 5.4_x86
        101739-17 5.3
        102423-07 4.1.4
        101665-10 4.1.3_U
```

The CERT Coordination Center thanks Eric Allman, AUSCERT, Terry Kyriacopoulos of Interlog Internet Services, and Dan Bernstein of the University of Illinois, Chicago for their contributions to the development of this advisory.

Revision History

```
Oct. 20, 1997  Appendix A - updated vendor information for Sun.
Sep. 24, 1997  Updated copyright statement

Dec. 20, 1996  Appendix A, Cray - added vendor information.
```