CERT Advisory CA-1995-05 Sendmail Vulnerability

==========
CA-93:16 CERT Advisory
November 4, 1993
Sendmail Vulnerability

- ----------

*** SUPERSEDED BY CA-95:05 ***

The CERT Coordination Center is working on eliminating a vulnerability in sendmail(8). This vulnerability potentially affects all systems running sendmail.

CERT is working with the vendor community to address this vulnerability. At this time, there are no known patches available for any vendor implementation that fully address this vulnerability. Until there is complete vendor information, CERT recommends that all implementations of sendmail be considered susceptible.

This advisory supersedes the sendmail portion of the CERT advisory (CA-93:15) of October 21, 1993.

CERT will continue to work with the vendors and will alert the community when patches become available.

Included with this advisory is an appendix describing tips that can be used by system administrators who are concerned about the possible exploitation of this vulnerability at their site.

- ----------

I. Description

A vulnerability exists in most versions of sendmail that allows unauthorized remote or local users to execute programs as any system user other than root.

This vulnerability affects the final destination sendmail host and can be exploited through an intermediate mail machine. Therefore, all sendmail recipient machines within a domain are potentially vulnerable.

II. Impact

Anyone (remote or local) can execute programs on the affected hosts as any userid other than root.

III. Approaches

CERT suggests three possible approaches to this problem. Although these approaches address all known aspects of this vulnerability, they are suggested only until vendor patches for this sendmail vulnerability are available.

Familiarity with sendmail and its installation and configuration, is recommended before implementing these modifications.

In order to protect your entire site it is necessary to apply the selected approach to *ALL* systems running sendmail at the site, and not just the mail hub.

A. Approach 1

This approach involves modifying the sendmail configuration to restrict the sendmail program mailer facility.

To restrict sendmail's program mailer facility, obtain and install the sendmail restricted shell program (smrsh 1.2) by Eric Allman (the original author of sendmail), following the directions included with the program.

1. Where to obtain the program

Copies of this program may be obtained via anonymous FTP from info.cert.org, in the /pub/tools/smrsh directory, or via anonymous FTP from ftp.uu.net in the /pub/security/smrsh directory.

Checksum information:

```
                    BSD Sum
30114 5 README
25757 2 smrsh.8
46786 5 smrsh.c

                  System V Sum
56478 10 README
42281 4 smrsh.8
65517 9 smrsh.c

                  MD5 Checksum
MD5 (README) = fc4cf266288511099e44b664806a5594
MD5 (smrsh.8) = 35aeefba9714f251a3610c7b1714e355
MD5 (smrsh.c) = d4822ce7c273fc8b93c68e39ec67739c
```

2. Impacts of this approach

While this approach allows a site to specify which programs can be run by sendmail (e.g. vacation(1)), attempts to invoke programs that are not included in the allowed set, or attempts using shell meta-characters (see smrsh program listing for a complete set of disallowed characters), will fail, resulting in log output to the syslog(3) facility. Programs that are specified in a site's /etc/aliases file should be considered for inclusion in the allowable program list.

Since .forward files allow user-specified programs to be run by sendmail, a survey of the contents of the system's .forward files may be required to prevent failure to deliver user mail.

```
*** WARNING ************************************************
* It is very important that sites *NOT* include interpreter   *
* programs (e.g. /bin/sh, /bin/csh, /bin/perl, /bin/uudecode, *
* /bin/sed, ...) in the list of allowed programs.             *
************************************************************
```

B. Approach 2

Like approach 1, this approach involves modifying the sendmail configuration. However, this approach completely disables the sendmail program mailer facility. This is a drastic, but quick action that can be taken while a site installs one of the other suggestions. Before implementing this approach, save a copy of the current sendmail configuration file.

To implement this approach edit the sendmail.cf file:

change from:

```
Mprog,  P=/bin/sh,      F=slFDM,        S=10,   R=20,   A=sh -c $u
```

to:

```
Mprog, P=/bin/false,    F=,     S=10,   R=20,   A=
```

Any changes to the sendmail.cf file will require that the sendmail process be restarted to ensure that the new configuration is used. See item 3 in Appendix A for more details.

1. Impacts of this approach

Attempts to invoke programs through sendmail will not be successful.

C. Approach 3

To the best of our knowledge, Eric Allman's public domain implementation of sendmail, sendmail 8.6.4, does not appear to be susceptible to this vulnerability. A working solution would then be to replace a site's sendmail, with sendmail 8.6.4.

1. Where to obtain the program

Copies of this version of sendmail may be obtained via anonymous FTP from ftp.cs.berkeley.edu in the /ucb/sendmail directory.

Checksum information:

```
                    BSD Sum
sendmail.8.6.4.base.tar.Z:      07718 428
```

```
sendmail.8.6.4.cf.tar.Z:        28004 179
sendmail.8.6.4.misc.tar.Z:      57299 102
sendmail.8.6.4.xdoc.tar.Z:      33954 251

                System V Sum
64609 856 sendmail.8.6.4.base.tar.Z
42112 357 sendmail.8.6.4.cf.tar.Z
8101 203 sendmail.8.6.4.misc.tar.Z
50037 502 sendmail.8.6.4.xdoc.tar.Z

                MD5 Checksum
MD5 (sendmail.8.6.4.base.tar.Z) = 59727f2f99b0e47a74d804f7ff654621
MD5 (sendmail.8.6.4.cf.tar.Z) = cb7ab7751fb8b45167758e9485878f6f
MD5 (sendmail.8.6.4.misc.tar.Z) = 8eaa6fbe9e9226667f719af0c1bde755
MD5 (sendmail.8.6.4.xdoc.tar.Z) = a9da24e504832f21a3069dc2151870e6
```

2. Impacts of this workaround

   Depending upon the currently installed sendmail program, switching to a different sendmail may require significant effort for the system administrator to become familiar with the new program. The site's sendmail configuration file may require considerable modification in order to provide existing functionality. In some cases, the site's sendmail configuration file may be incompatible with the sendmail 8.6.4 configuration file.

- ----------
The CERT Coordination Center wishes to thank the members of the following response teams for their assistance in analyzing and testing both the problem and the solutions: SERT, ASSIST, CIAC, and DFN-CERT. CERT would especially like to thank Eric Allman, Matt Blaze, Andy Sherman, Gene Spafford, Tim Seaver, and many others who have provided technical assistance with this effort.
- ----------

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 via anonymous FTP from info.cert.org.

Appendix A

This appendix describes tips that can be used by system administrators who are concerned about the possible exploitation of this vulnerability at their site.

There are two actions that can be taken by system administrators to try to detect the exploitation of this vulnerability at their sites.

- Examine all bounced mail to look for unusual occurrences.
- Examine syslog files for unusual occurrences of "|" characters

In order to do this, sendmail must be configured to direct bounced mail to the postmaster (or other designated person who will examine the bounced mail). Sendmail must also be configured to provide adequate logging.

1) To direct bounced mail to the postmaster, place the following entry in the options part of the general configuration information section of the sendmail.cf file.

   ```
   # Cc my postmaster on error replies I generate
   OPpostmaster
   ```

2) To set sendmail's logging level, place the following entry in the options part of the general configuration information section of the sendmail.cf

file. Note that the logging level should be 9 or higher in order to provide
adequate logging.

```
# log level
OL9
```

3) Once changes have been made in the sendmail configuration file,
it will be necessary to kill all existing sendmail processes,
refreeze the configuration file (if needed - see the note below),
and restart the sendmail program.

Here is an example from SunOS 4.1.2:

As root:

```
# /usr/bin/ps -aux | /usr/bin/grep sendmail
root 130  0.0  0.0  168    0 ?  IW   Oct  2  0:10 /usr/lib/sendmail -bd -q
# /bin/kill -9 130               (kill the current sendmail process)
# /usr/lib/sendmail -bz          (create the configuration freeze file)
# /usr/lib/sendmail -bd -q30m    (run the sendmail daemon)
```

**Note: Some sites do not use frozen configuration files and some do. If
your site is using frozen configuration files, there will be a file
named sendmail.fc in the same directory as the sendmail configuration
file (sendmail.cf).


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

iQA/AwUBOBS95Fr9kb5qlZHQEQK4vQCgsC7r8Ca14M/H5J7xNIIRhjokfYAAoN02
Af5uDmzrQvzMi89dU4mMB0aB
=cFVH
-----END PGP SIGNATURE-----
```