CERT Advisory CA-1997-14 Vulnerability in metamail

Original issue date: May 21, 1997
Last revised: October 25, 1999
Added vendor information for Data General.

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

The CERT Coordination Center has received reports of a vulnerability in metamail, a program that implements MIME. By exploiting the vulnerability, a sender of a MIME-encoded electronic mail message can cause the receiver of the message to execute an arbitrary command if the receiver processes the message using the metamail package. If the attacker has an account on the target user's local system or if the target user's system supports AFS or another distributed filesystem, then the attacker can arrange for the arbitrary command to be one the attacker created. This affects versions of metamail through 2.7 (the current version).

The CERT/CC team recommends installing a vendor patch, if one is available, patching metamail yourself, or disabling metamail (see Section III).

We will update this advisory as we receive additional information. Please check our advisory files regularly for updates that relate to your site.

I. Description

Multipurpose Internet Mail Extensions (MIME) is a standard format for extended Internet electronic mail. The MIME format permits email to include enhanced text, graphics, and audio in a standardized and interoperable manner. MIME is described in RFCs 2045 through 2049.

metamail is a package that implements MIME (note: metamail can be obtained from ftp://ftp.funet.fi/pub/unix/mail/metamail/mm2.7.tar.Z). Using a configurable "mailcap" file, metamail determines how to treat blocks of electronic mail text based on the content as described by email headers. Some popular packages for handling electronic mail have hooks that allow metamail to be called automatically while a message is being processed.

A condition exists in metamail in which there is insufficient variable checking in some support scripts. By carefully crafting appropriate message headers, a sender can cause the receiver of the message to execute an arbitrary command if the receiver processes the message using the metamail package.

II. Impact

A sender of a MIME encoded mail message can cause the receiver to execute an arbitrary command. If the attacker has an account on the target user's local system or if the target user's system supports AFS or another distributed filesystem, then the attacker can arrange for the arbitrary command to be one the attacker created.

III. Solution

If your vendor supplies metamail with its distribution, then install a patch from your vendor (Solution A). If your vendor does not distribute metamail with their products or does not have a patch available, use the workaround in Solution B. An alternative for those with sufficient expertise is to patch the metamail scripts as described in Solution C.

A. Install a patch from your vendor, if appropriate

The vendors we have heard from so far are listed below, with details in Appendix A. We will update the appendix as we receive more information.

Berkeley Software Design, Inc. (BSDI)
Cray Research - A Silicon Graphics Company
Digital Equipment Corporation
FreeBSD, Inc.
Hewlett-Packard Company
IBM Corporation
Linux
NEC Corporation
Silicon Graphics Inc.
Solbourne
Sun Microsystems, Inc.

B. Disable metamail scripts

To disable the metamail scripts, remove the execute permissions from the scripts that are located in the mm2.7/src/bin directory of metamail v2.7 (the latest version of metamail). Remember that, depending on your installation of metamail, the scripts may be located in other directories in your operating system.

C. Patch metamail yourself

Sites that need to use metamail and have the expertise may wish to patch the scripts that are part of the metamail distribution. Note that the guidance below is supplied as is, and you need to be sure that you understand the impact (if any) that your modifications will have on metamail functionality.

The scripts referred to in the following material are all located in the mm2.7/src/bin directory of metamail v2.7 (the latest version of metamail). They may be located in other directories in your operating system.

1. Ensure that parameters supplied to the scripts do not contain anywhite space.

Using showexternal as an example, add the following code before any argument processing:

```
# Check argument integrity. Don't trust mail headers
switch ("$1$2$3$4$5$6$7")
case "*[\t ]*":
 echo "Illegal white space in arguments\!"
 echo "Command was:"
 echo "'$0' '$1' '$2' '$3' '$4' '$5' '$6' '$7'"
 exit 2
endsw
```

Add this code to the showexternal script at the very least, prior to any argument processing within that script. We encourage you to add this code to other scripts in mm2.7/src/bin directory to ensure that arguments in those scripts also exclude white space. You may need to adapt the code for your particular system.

Note that this patch may affect functionality in cases (such as filenames) where parameters may have legitimately included white space.

This step addresses the problem referred to in this advisory. As part of a more generally secure programming practice, please also consider the following modifications.

2. Ensure that script parameter references are quoted. For instance, in show external, change this line:

set name=$3

to

set name="$3"

This should be done for every reference to a command line argument in each of the scripts.

Note that csh has a :q operator which is also intended for this purpose. If you prefer, you can use this operator in each case instead of quoting.

3. Any variables in these scripts that take their value (either directlyor indirectly) from a script parameter should also be quoted where necessary.

For instance, in the showexternal script, change the line:

```
get $name $NEWNAME
```

to

```
get "$name" "$NEWNAME"
```

Also change the following line:

```
if ($NEWNAME != $name) then
```

to

```
if ("$NEWNAME" != "$name") then
```

Similarly, there will be other instances where $name specifically, and other variables in general, should be quoted.

The reason is that these variables take their value from the script parameters (for example, $name takes its value from $3, and $NEWNAME may take its value from $name).

As before, the :q operator can be used in each case.

Note that in doing this step, some care will be required.

4. Make sure that users have an appropriate umask set for directory and file creation.

Although the value is subject to local restrictions, you may want to use a default value of 027 (depending upon the local environment).

5. Make sure that users have an appropriate value set for the environment variable METAMAIL_TMPDIR.

This environment variable tells metamail where to create the temporary files it needs while processing. If the variable is not set in the user's environment, the default value is /tmp. Since /tmp is accessible by all users, it is possible that use of this value will allow exploitation of race conditions. We recommend setting the value to a protected directory belonging to the user.

6. To ensure that the METAMAIL_TMPDIR is used properly and in a secure manner, consider modifications along the following lines, using the showexternal scripts as an example.

These modifications should reflect and reinforce the suggestions outlined in the previous two items, namely that the temporary directory metamail uses should be protected and accessible only by the user.

Note that the following code fragments are for example only, and sites should adapt this code according to local requirements.

Change these lines:

```
if (! $?METAMAIL_TMPDIR) then
 set METAMAIL_TMPDIR=/tmp
endif

to

# Set a sensible value for the temporary directory, if its not
# already set. If TMPDIR is set previously, then we will
# assume it is adequately protected.
if (! $?METAMAIL_TMPDIR) then
 if ($?TMPDIR) then
 set METAMAIL_TMPDIR="$TMPDIR"
 else
 set METAMAIL_TMPDIR=~/metamail_tmp
 endif
endif

# Set a sensible umask value
umask 077

# Make sure that the temporary directory is available
if (! -d "$METAMAIL_TMPDIR") then

 if (! -e "$METAMAIL_TMPDIR") then
 mkdir "$METAMAIL_TMPDIR"
 else
 echo "$METAMAIL_TMPDIR exists, but is not a directory"
 exit 2
 endif

 if ( $status != 0 || ! -d "$METAMAIL_TMPDIR" ) then
 echo "Error creating $METAMAIL_TMPDIR"
 exit 2
 endif

endif
```

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 or use the workaround in Section III.

Berkeley Software Design, Inc. (BSDI)

BSDI ships metamail and is vulnerable to the attack. Patches are in progress.

Cray Research - A Silicon Graphics Company

Cray Research does not ship metamail as part of either Unicos or Unicos/mk.

Data General

Our metamail scripts are Bourne shell scripts from the SVR4.2MP distribution and do not have the parameter quoting problem.

Digital Equipment Corporation

Digital Equipment Corporation
Software Security Response Team
May 19,1997

This reported problem is not present for Digital's ULTRIX or Digital UNIX Operating Systems Software.

- DIGITAL EQUIPMENT CORPORATION

FreeBSD, Inc.

If you installed the metamail package or port then you are vulnerable. All released versions of FreeBSD including 2.2.2R have this flaw in them. The port was corrected as of May 21, 1997. Either update your system from a more recent port, or apply the patches contained in this advisory to those files affected.

Hewlett-Packard Company

HP-UX is vulnerable; patches are in progress.

IBM Corporation

Not vulnerable, metamail is not shipped as part of AIX.

Linux

Debian:

Debian uses its own bourne shell based metamail scripts not the standard ones.

Red Hat: i386
rpm -Uvh ftp://ftp.redhat.com/updates/4.2/i386/metamail-2.7-7.1.i386.rpm

Alpha
rpm -Uvh ftp://ftp.redhat.com/updates/4.2/alpha/metamail-2.7-7.1.alpha.rpm

NEC Corporation

UX/4800	Not vulnerable for all versions.
EWS-UX/V(Rel4.2MP)	Not vulnerable for all versions.
EWS-UX/V(Rel4.2)	Not vulnerable for all versions.
UP-UX/V(Rel4.2MP)	Not vulnerable for all versions.
EWS-UX/V(Rel4.0)	Not vulnerable for all versions.
UP-UX/V	Not vulnerable for all versions.

Silicon Graphics Inc.

At this time, Silicon Graphics does not have any public information for the metamail issue. Silicon Graphics has communicated with CERT and other external security parties and is actively investigating this issue. When more Silicon Graphics information (including any possible patches) is available for release, that information will be released via the SGI security mailing list, wiretap.

For subscribing to the wiretap mailing list and other SGI security related information, please refer to the Silicon Graphics Security Headquarters website located at:

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

Solbourne

We do not ship the utility.
We do not anticipate providing a patch, since we do not ship the utility.

Sun Microsystems, Inc.

Sun does not ship metamail with any of our platforms.
Sun has no plans to produce patches.

The CERT Coordination Center staff thanks Olaf Kirch for contributing code to the solution section and thanks BSDI and FreeBSD for their input on the solution.

Revision History

```
Oct 25, 1999 Added vendor information for Data General.
Oct 29, 1997 Updated vendor information for Red Hat.
Sep 30, 1997 Updated copyright statement
May 23, 1997 Appendix A, BSDI - added information.
May 21, 1997 Appendix A, FreeBSD - changed release date of the patch
```