CERT Advisory CA-1991-01a REVISED SunOS /bin/mail Vulnerability

CA-91:01a CERT Advisory
February 22, 1991
REVISED SunOS /bin/mail Vulnerability

- ---

*** THIS ADVISORY HAS BEEN SUPERSEDED BY CA-95:02 ***

The Computer Emergency Response Team/Coordination Center (CERT/CC) has received the following information from Sun Microsystems, Inc. (Sun). Sun has given the CERT/CC permission to distribute their Security Bulletin. It contains information regarding a fix for a vulnerability in SunOS 4.0.3, SunOS 4.1 and SunOS 4.1.1.

An important piece of information was missing from the Sun Security Bulletin #00105 which was included in the CA-91:01 CERT Advisory on this same subject. After the old /bin/mail has been renamed, it is important to remove the setuid root bit. Sun also suggests that the protection bits on the new /bin/mail to be set to 4111 instead of 4755.

The CERT/CC advises that the /bin/mail.old file be removed once the new /bin/mail is in place and verified that it is functioning correctly.

This is from the original Sun Security Bulletin #00105:

```
           AS ROOT:

           # mv /bin/mail to /bin/mail.old
           # cp $arch/$os/mail to /bin/mail
            (where $arch is either sun3 sun4 sun4c or sun3x)
            (and where $os is either 4.0.3 4.1 or 4.1.1)
            ( change the permissions for the newly installed mail)
           # chmod 4755 /bin/mail
```

In CERT's opinion, the CERT Advisory should have the following information.

```
           AS ROOT:

           # mv /bin/mail to /bin/mail.old
  new->    # chmod 400 /bin/mail.old
           # cp $arch/$os/mail to /bin/mail
            (where $arch is either sun3 sun4 sun4c or sun3x)
            (and where $os is either 4.0.3 4.1 or 4.1.1)
            ( change the permissions for the newly installed mail)
updated -> # chmod 4111 /bin/mail
```

The complete Sun Security Bulletin #00105 is being resent including the CERT/CC changes.

For more information, please contact Sun Microsystems at 1-800-USA-4SUN.

- ---

SUN MICROSYSTEMS SECURITY BULLETIN:
#00105

==========

All of these patches are available through your local Sun answer centers worldwide. As well as through anonymous ftp to ftp.uu.net in the ~ftp/sun-dist directory.

Please refer to the Sun BugID and PatchID when requesting patches from Sun answer centers.

NO README information will be posted in the patch on UUNET. Please refer

the the information below for patch installation instructions.
==

Sun Bug ID : 1047340
Synopsis   : /bin/mail can be caused to invoke a root shell if given the
              (im)proper arguments.
Sun Patch ID: 100224-01
Checksum of compressed tarfile 100224-01.tar.Z = 64102   109

==

Patch-ID# 100224-01
Keywords: mail, delivery, /bin/mail, 4.1, sendmail
Synopsis: SunOS 4.1.1, 4.1, 4.0.3: program "mail" problem in delivering
          mail + security enhancement
Date: 15 Jan 1990

SunOS release: 4.0.3 4.1 4.1.1

Topic: /bin/mail delivering fix

BugId's fixed with this patch: 1045636 1047340

Architectures for which this patch is available: sun3, sun3x, sun4, sun4c,
sun4/490_4.1_PSR_A.

Patches which may conflict with this patch: 100161-01. This patch obsoletes
                                            patch 100161-01 since this patch
                                            incorporates 100161-01 fixes plus
                                            the new fixes.
Obsoleted by: SysV Release 4

Problem Description:

Bug ID: 1045636

 /bin/mail is the local delivery agent for sendmail. In
some particular instance, /bin/mail parse its argument incorrectly
and therefore, mail are being drop into the bit bucket...

If you have users that has "f" has the second character, you might want
to try the following: (substitute "af" with anyuser with "f" as second
character)

>From any machine except mailhost:

/bin/lib/sendmail -t -v <<END
From: anyuser
to: anyuser
Subject: test
Cc: af   <-- substitute any username with second character as "f"
test

END

When the mail arrived on mailhost, sendmail process will invoke
/bin/mail with the following argument "/bin/mail -r anyuser -d af
anyuser". Now you are in trouble. The following are different
scenarios for /bin/mail.

1) /bin/mail -r anyuser -d af <mailmessages   worked fine
2) /bin/mail -r anyuser -d anyone af ... <mailmessages worked fine
3) /bin/mail -r anyuser -d af anyone ... <mailmessages !!error!!

    in case (3), /bin/mail thinks that you want to read mail instead of
    delivering mail. Therefore, mail messages is lost.

BugID: 1047340

/bin/mail can be caused to invoke a root shell if given the
        (im)proper arguments.

INSTALL:

AS ROOT:

mv /bin/mail to /bin/mail.old
chmod 400 /bin/mail.old
cp $arch/$os/mail to /bin/mail
 (where $arch is either sun3 sun4 sun4c or sun3x)
 (and where $os is either 4.0.3 4.1 or 4.1.1)
 (change the permissions for the newly installed mail)
chmod 4111 /bin/mail

- --
Computer Emergency Response Team/Coordination Center (CERT/CC)
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890

Internet E-mail: cert@cert.org
Telephone: 412-268-7090 24-hour hotline:
           CERT personnel answer 7:30a.m.-6:00p.m. EST.
           On call for emergencies during other hours.

Past advisories and other computer security related information are available
for anonymous ftp from the cert.org (192.88.209.5) system.

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

iQA/AwUBOBS9lFr9kb5qlZHQEQJpWACfZ5yYpqgpdRSXuBqjmtkv85nad78AoPXQ
joXDjXK9WlT3SYwd9/rKCpsq
=y7Gz
-----END PGP SIGNATURE-----