

FreeBSD Security Advisory

FreeBSD-SA-03:11.sendmail

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2003-08/0215.html>

From: FreeBSD Security Advisories (security-advisories_at_freebsd.org)

Date: 08/26/03

Date: Tue, 26 Aug 2003 09:43:31 -0700 (PDT)

To: FreeBSD Security Advisories <security-advisories@freebsd.org>

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

=====
FreeBSD-SA-03:11.sendmail Security Advisory
The FreeBSD Project

Topic: sendmail DNS map problem

Category: contrib

Module: contrib_sendmail

Announced: 2003-08-26

Credits: Oleg Bulyzhin <oleg@rinet.ru>

Affects: 4.6-RELEASE (up to -p16), 4.7-RELEASE (up to -p13),
4.8-RELEASE (up to -p3), 5.0-RELEASE (up to -p11)
4-STABLE prior to Mar 29 19:33:18 2003 UTC

Corrected: 2003-08-25 22:33:14 UTC (RELENG_5_0)
2003-08-25 22:35:23 UTC (RELENG_4_8)
2003-08-25 22:36:10 UTC (RELENG_4_7)
2003-08-25 22:38:53 UTC (RELENG_4_6)

FreeBSD only: NO

For general information regarding FreeBSD Security Advisories, including descriptions of the fields above, security branches, and the following sections, please visit
<URL:<http://www.freebsd.org/security/>>.

I. Background

FreeBSD includes sendmail(8), a general purpose internet network mail routing facility, as the default Mail Transfer Agent (MTA).

II. Problem Description

Some versions of sendmail (8.12.0 through 8.12.8) contain a programming error in the code that implements DNS maps. A malformed DNS reply packet may cause sendmail to call `free()` on an uninitialized pointer.

NOTE: The default sendmail configuration in FreeBSD does not utilize DNS maps.

III. Impact

Calling `free()` on an uninitialized pointer may result in a sendmail child process crashing. It may also be possible for an attacker to somehow influence the value of the `uninitialized pointer' and cause an arbitrary memory trunk to be freed. This could further lead to some other exploitable vulnerability, although no such cases are known at this time.

IV. Workaround

Do not use DNS maps.

V. Solution

Do one of the following:

1) Upgrade your vulnerable system to 4–STABLE, 5.1–RELEASE, or to the RELENG_5_1, RELENG_4_8, or RELENG_4_7 security branch dated after the correction date (5.1–RELEASE–p11, 4.8–RELEASE–p4, or 4.7–RELEASE–p14, respectively).

2) To patch your present system:

The following patch has been verified to apply to FreeBSD 5.0, 4.8, 4.7, and 4.6 systems.

a) Download the relevant patch from the location below, and verify the detached PGP signature using your PGP utility.

<ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-03:11/sendmail.patch>
<ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-03:11/sendmail.patch.asc>

b) Execute the following commands as root:

```
# cd /usr/src
# patch < /path/to/patch
# cd /usr/src/lib/libsm
# make obj && make depend && make
# cd /usr/src/lib/libsmutil
# make obj && make depend && make
# cd /usr/src/usr.sbin/sendmail
# make obj && make depend && make && make install
```

c) Restart sendmail. Execute the following command as root.

```
# /bin/sh /etc/rc.sendmail restart
```

VI. Correction details

The following list contains the revision numbers of each file that was corrected in FreeBSD.

Path Revision
Branch

src/UPDATING

RELENG_5_0 1.229.2.17
RELENG_4_8 1.73.2.80.2.6
RELENG_4_7 1.73.2.74.2.17
RELENG_4_6 1.73.2.68.2.45

src/sys/conf/newvers.sh

RELENG_5_0 1.48.2.12
RELENG_4_8 1.44.2.29.2.5
RELENG_4_7 1.44.2.26.2.16
RELENG_4_6 1.44.2.23.2.34

src/contrib/sendmail/src/sm_resolve.c

RELENG_5_0 1.1.1.4.2.1
RELENG_4_8 1.1.1.1.2.2.4.1
RELENG_4_7 1.1.1.1.2.2.2.1
RELENG_4_6 1.1.1.1.2.1.2.2

VII. References

<URL:<http://www.sendmail.org/dnsmap1.html>>

<URL:<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0688>>

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v1.2.2 (FreeBSD)

iD8DBQE/S4xUFdaIBMps37IRAoJ4AJ9AiL4AMISXz/thD2SuNkKSQsUZHgCeKbds
qEb9Em5EIZZOEnIajwneKIg=
=SjNG

-----END PGP SIGNATURE-----

freebsd–security@freebsd.org mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd–security>

To unsubscribe, send any mail to "freebsd–security–unsubscribe@freebsd.org"