

FreeBSD Security Advisory

FreeBSD-SA-04:11.msync

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2004-05/0105.html>

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

Date: 05/26/04

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

Date: Wed, 26 May 2004 13:32:51 +0200 (CEST)

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

Hash: SHA1

=====
FreeBSD-SA-04:11.msync Security Advisory
The FreeBSD Project

Topic: buffer cache invalidation implementation issues

Category: core

Module: sys

Announced: 2004-05-26

Credits: Stephan Uphoff <ups@tree.com>

Matt Dillon <dillon@apollo.backplane.com>

Affects: All FreeBSD versions prior to the correction date

Corrected: 2004-05-25 22:46:38 UTC (RELENG_4, 4.10-STABLE)

2004-05-25 23:07:55 UTC (RELENG_5_2, 5.2.1-RELEASE-p8)

2004-05-22 23:09:19 UTC (RELENG_4_10, 4.10-RELEASE)

2004-05-25 23:01:21 UTC (RELENG_4_9, 4.9-RELEASE-p9)

2004-05-25 23:01:19 UTC (RELENG_4_8, 4.8-RELEASE-p22)

CVE Name: CAN-2004-0435

FreeBSD only: YES

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

The msync(2) system call is used by applications to request that modified memory pages are written to permanent storage.

II. Problem Description

Programming errors in the implementation of the msync(2) system call involving the MS_INVALIDATE operation lead to cache consistency problems between the virtual memory system and on–disk contents.

III. Impact

In some situations, a user with read access to a file may be able to prevent changes to that file from being committed to disk.

IV. Workaround

There is no workaround.

V. Solution

Perform one of the following:

1) Upgrade your vulnerable system to 4–STABLE; or to the RELENG_5_2, RELENG_4_10, RELENG_4_9, or RELENG_4_8 security branch dated after the correction date.

2) To patch your present system:

The following patches have been verified to apply to FreeBSD 4.8, 4.9, 4.10 and 5.2 systems.

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

[FreeBSD 5.2]

```
# fetch ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-04:11/msync5.patch  
# fetch ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-04:11/msync5.patch.asc
```

[FreeBSD 4.8, 4.9, 4.10]

```
# fetch ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-04:11/msync4.patch  
# fetch ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-04:11/msync4.patch.asc
```

b) Apply the patch.

```
# cd /usr/src  
# patch < /path/to/patch
```

c) Recompile your kernel as described in <http://www.freebsd.org/handbook/kernelconfig.html> and reboot the system.

VI. Correction details

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

FreeBSD–Security: FreeBSD Security Advisory FreeBSD–SA–04:11.msync

Branch Revision
Path

RELENG_4

src/sys/ufs/ufs/ufs_readwrite.c 1.65.2.16
src/sys/vm/vm_map.c 1.187.2.30

RELENG_4_10

src/sys/ufs/ufs/ufs_readwrite.c 1.65.2.14.4.1
src/sys/vm/vm_map.c 1.187.2.24.2.4

RELENG_4_9

src/UPDATING 1.73.2.89.2.10
src/sys/conf/newvers.sh 1.44.2.32.2.10
src/sys/ufs/ufs/ufs_readwrite.c 1.65.2.14.2.1
src/sys/vm/vm_map.c 1.187.2.23.2.1

RELENG_4_8

src/UPDATING 1.73.2.80.2.25
src/sys/conf/newvers.sh 1.44.2.29.2.23
src/sys/ufs/ufs/ufs_readwrite.c 1.65.2.13.2.1
src/sys/vm/vm_map.c 1.187.2.17.2.1

RELENG_5_2

src/UPDATING 1.282.2.16
src/sys/conf/newvers.sh 1.56.2.15
src/sys/ufs/ufs/ufs_vnops.c 1.119.2.1
src/sys/vm/vm_object.c 1.317.2.1

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

Version: GnuPG v1.2.4 (FreeBSD)

iD8DBQFAH2pFdaIBmps37IRAmycAJ0cv/iG6NIGBsC1xT4gg/Gx3IF8DwCghfHl
G2wdUNyfvhz0u3kFB9pH41c=
=SK1u

-----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"