

# FreeBSD Security Advisory FreeBSD–SA–05:07.Idt

*Source:* <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2005-05/0005.html>

---

**From:** FreeBSD Security Advisories (*security-advisories\_at\_freebsd.org*)

**Date:** 05/06/05

Date: Fri, 6 May 2005 03:03:13 GMT

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

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

Hash: SHA1

=====  
FreeBSD–SA–05:07.Idt Security Advisory  
The FreeBSD Project

Topic: Local kernel memory disclosure in i386\_get\_ldt

Category: core

Module: sys\_i386

Announced: 2005–05–06

Credits: Christer Oberg

Affects: All FreeBSD/i386 4.x releases since 4.7–RELEASE

All FreeBSD/i386 5.x and FreeBSD/amd64 5.x releases  
prior to 5.4–RELEASE

Corrected: 2005–05–06 02:40:19 UTC (RELENG\_5, 5.4–STABLE)

2005–05–06 02:40:49 UTC (RELENG\_5\_4, 5.4–RELEASE)

2005–05–06 02:40:32 UTC (RELENG\_5\_3, 5.3–RELEASE–p12)

2005–05–06 02:39:35 UTC (RELENG\_4, 4.11–STABLE)

2005–05–06 02:40:05 UTC (RELENG\_4\_11, 4.11–RELEASE–p6)

2005–05–06 02:39:52 UTC (RELENG\_4\_10, 4.10–RELEASE–p11)

CVE Name: CAN–2005–1400

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 `i386_get_ldt(2)` system call allows a process to request that a  
portion of its Local Descriptor Table be copied from the kernel into  
userland.

## II. Problem Description

The `i386_get_ldt(2)` syscall performs insufficient validation of its input arguments. In particular, negative or very large values may allow inappropriate data to be copied from the kernel.

### III. Impact

Kernel memory may be disclosed to the user process. Such memory might contain sensitive information, such as portions of the file cache or terminal buffers. This information might be directly useful, or it might be leveraged to obtain elevated privileges in some way. For example, a terminal buffer might include a user–entered password.

### IV. Workaround

No workaround is known for i386 and amd64 systems; other platforms are not affected by this issue.

### V. Solution

Perform one of the following:

1) Upgrade your vulnerable system to 4–STABLE or 5–STABLE, or to the `RELENG_5_3`, `RELENG_4_11`, or `RELENG_4_10` security branch dated after the correction date.

2) To patch your present system:

The following patches have been verified to apply to FreeBSD 4.10, 4.11, and 5.3 systems.

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

[FreeBSD 4.x]

```
# fetch ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:07/ldt4.patch  
# fetch ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:07/ldt4.patch.asc
```

[FreeBSD 5.x]

```
# fetch ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:07/ldt5.patch  
# fetch ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:07/ldt5.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.

Branch Revision  
Path

---

RELENG\_4  
src/sys/i386/i386/sys\_machdep.c 1.47.2.4  
RELENG\_4\_11  
src/UPDATING 1.73.2.91.2.7  
src/sys/conf/newvers.sh 1.44.2.39.2.10  
src/sys/i386/i386/sys\_machdep.c 1.47.2.3.8.1  
RELENG\_4\_10  
src/UPDATING 1.73.2.90.2.12  
src/sys/conf/newvers.sh 1.44.2.34.2.13  
src/sys/i386/i386/sys\_machdep.c 1.47.2.3.6.1  
RELENG\_5  
src/sys/i386/i386/sys\_machdep.c 1.92.2.3  
RELENG\_5\_4  
src/UPDATING 1.342.2.24.2.6  
src/sys/i386/i386/sys\_machdep.c 1.92.2.1.2.1  
RELENG\_5\_3  
src/UPDATING 1.342.2.13.2.15  
src/sys/conf/newvers.sh 1.62.2.15.2.17  
src/sys/i386/i386/sys\_machdep.c 1.92.4.1

---

The latest revision of this advisory is available at  
<ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-05:07.ltd.asc>

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

Version: GnuPG v1.4.1 (FreeBSD)

iD8DBQFCetz/FdaIBMps37IRAsGyAJ0e/186b85KV2w0iqXy+eZe4aoGMwCfSIRm  
TqqVUL/yrYbXxlyzJZNEjPs=  
=/YXX

-----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"