

# FreeBSD Security Advisory

## FreeBSD-SA-08:04.ipsec

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2008-02/msg00018.html>

---

- *From:* FreeBSD Security Advisories <[security-advisories@xxxxxxxxxxx](mailto:security-advisories@xxxxxxxxxxx)>
  - *Date:* Thu, 14 Feb 2008 12:11:30 GMT
- 

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

Hash: SHA1

=====  
FreeBSD-SA-08:04.ipsec Security Advisory  
The FreeBSD Project

Topic: IPsec null pointer dereference panic

Category: core

Module: ipsec

Announced: 2008-02-14

Credits: Takashi Sogabe, Tatyua Jinmei

Affects: FreeBSD 5.5

Corrected: 2008-02-14 11:49:39 UTC (RELENG\_5, 5.5-STABLE)

2008-02-14 11:50:28 UTC (RELENG\_5\_5, 5.5-RELEASE-p19)

CVE Name: CVE-2008-0177

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

### I. Background

The IPsec suite of protocols provide network level security for IPv4 and IPv6 packets. FreeBSD includes software originally developed by the KAME project which implements the various protocols that make up IPsec.

### II. Problem Description

There is an improper reference to a data structure in the processing of IPsec packets, which can result in a NULL pointer being dereferenced.

### III. Impact

A single specifically crafted IPv6 packet could cause the kernel to panic, when the kernel had been configured to process IPsec and IPv6 traffic.

This requires IPSEC to be compiled into the kernel, it does not necessarily have to be configured at that point.

#### IV. Workaround

No workaround is available, but kernels which does not include IPsec support are not vulnerable. The GENERIC and SMP kernel configurations distributed with FreeBSD releases do not include IPsec support.

#### V. Solution

Perform one of the following:

- 1) Upgrade your vulnerable system to 5-STABLE, or to the RELENG\_5\_5 security branch dated after the correction date.
- 2) To patch your present system:

The following patches have been verified to apply to FreeBSD 5.5 systems.

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

```
# fetch http://security.FreeBSD.org/patches/SA-08:04/ipsec.patch  
# fetch http://security.FreeBSD.org/patches/SA-08:04/ipsec.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_5  
src/sys/netinet6/ipcomp_input.c 1.7.4.2  
RELENG_5_5  
src/UPDATING 1.342.2.35.2.20  
src/sys/conf/newvers.sh 1.62.2.21.2.21  
src/sys/netinet6/ipcomp_input.c 1.7.4.1.4.1
```

---

VII. References

<http://www.kb.cert.org/vuls/id/110947>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0177>

The latest revision of this advisory is available at

<http://security.FreeBSD.org/advisories/FreeBSD-SA-08:04.ipsec.asc>

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

Version: GnuPG v1.4.8 (FreeBSD)

iD8DBQFHtC0HFdaIBMps37IRAt5gAKCGnYEX3r7n0Dsypmfv2m1J9pgICwCfd6uH

Gy2w6OYNovnfrb7EN0jWCjM=

=jHy3

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

---

freebsd-security@xxxxxxxxxxx mailing list

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

To unsubscribe, send any mail to "freebsd-security-unsubscribe@xxxxxxxxxxx"