

# [UNIX] FreeBSD Kadmind Remote Heap Buffer Overflow

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-05/0026.html>

---

**From:** SecuriTeam (*support\_at\_securiteam.com*)

**Date:** 05/06/04

To: list@securiteam.com

Date: 6 May 2004 18:30:29 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

-----

FreeBSD Kadmind Remote Heap Buffer Overflow

---

## SUMMARY

A remotely exploitable heap overflow was found in FreeBSD's kadmind. Heimdal implements the Kerberos 5 authentication protocol. The kadmind provides the administrative interface to the Kerberos Key Distribution Center (KDC). In some configurations, Kerberos 4 support is present.

## DETAILS

### Vulnerable Systems:

- \* FreeBSD version 4 built with either Kerberos 4 or 5
- \* FreeBSD version 5 prior to 5.1 built with either Kerberos 4 or 5

### Immune Systems:

- \* FreeBSD 4 STABLE (dated after the correction date)
- \* FreeBSD RELENG\_4\_8 and RELENG\_4\_9 (dated after the correction date)

### CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0434>>  
CAN-2004-0434

## Securiteam: [UNIX] FreeBSD Kadmin Remote Heap Buffer Overflow

An input validation error was discovered in the k5admin code that handles the framing of Kerberos 4 compatibility administration requests. The code assumed that the length given in the framing was always two or more bytes. Smaller lengths will cause k5admin to read an arbitrary amount of data into a minimally sized buffer on the heap.

Note that this code is not present unless k5admin has been compiled with Kerberos 4 support. This will occur if a FreeBSD system is compiled with both of WITH\_KERBEROS4 and WITH\_KERBEROS5 build flags. These flags are never simultaneously set during the FreeBSD binary release process; consequently, binary installs of FreeBSD (even with Kerberos support installed) are not affected.

### Impact

A remote attacker can send a specially formatted message to the k5admin daemon that will cause it to either crash or end in arbitrary code execution.

### Workaround

Disable the Kerberos 4 support in k5admin by running it with the '--no-kerberos4' option.

### Solution

Perform one of the following:

1) Upgrade your vulnerable system to 4-STABLE; or to the 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 and 4.9.

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

```
# fetch
```

```
ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-04:09/kadmin.patch
```

```
# fetch
```

```
ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-04:09/kadmin.patch.asc
```

b) Execute the following commands as root:

```
# cd /usr/src
```

```
# patch < /path/to/patch
```

```
# cd /usr/src/kerberos5/tools
```

```
# make obj && make depend && make
```

```
# cd /usr/src/kerberos5/lib
```

```
# make obj && make depend && make
```

```
# cd /usr/src/kerberos5/libexec/k5admin
```

```
# make obj && make depend && make all install
```

Securiteam: [UNIX] FreeBSD Kadmind Remote Heap Buffer Overflow

ADDITIONAL INFORMATION

The information has been provided by <mailto:demidov@gleg.net> Evgeny Demidov.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

**DISCLAIMER:**

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.