

# FreeBSD Security Advisory

## FreeBSD-SA-08:05.openssh

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2008-04/msg00009.html>

---

- *From:* FreeBSD Security Advisories <[security-advisories@xxxxxxxxxxx](mailto:security-advisories@xxxxxxxxxxx)>
  - *Date:* Thu, 17 Apr 2008 00:14:55 GMT
- 

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

Hash: SHA1

=====  
FreeBSD-SA-08:05.openssh Security Advisory  
The FreeBSD Project

Topic: OpenSSH X11-forwarding privilege escalation

Category: contrib

Module: openssh

Announced: 2008-04-17

Credits: Timo Juhani Lindfors

Affects: All supported versions of FreeBSD

Corrected: 2008-04-16 23:58:33 UTC (RELENG\_7, 7.0-STABLE)

2008-04-16 23:58:52 UTC (RELENG\_7\_0, 7.1-RELEASE-p1)

2008-04-16 23:59:35 UTC (RELENG\_6, 6.3-STABLE)

2008-04-16 23:59:48 UTC (RELENG\_6\_3, 6.3-RELEASE-p2)

2008-04-17 00:00:04 UTC (RELENG\_6\_2, 6.2-RELEASE-p12)

2008-04-17 00:00:28 UTC (RELENG\_6\_1, 6.1-RELEASE-p24)

2008-04-17 00:00:41 UTC (RELENG\_5, 5.5-STABLE)

2008-04-17 00:00:54 UTC (RELENG\_5\_5, 5.5-RELEASE-p20)

CVE Name: CVE-2008-1483

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

OpenSSH is an implementation of the SSH protocol suite, providing an encrypted and authenticated transport for a variety of services, including remote shell access. The OpenSSH server daemon (sshd) provides support for the X11 protocol by binding to a port on the server and forwarding any connections which are made to that port.

### II. Problem Description

## FreeBSD Security Advisory FreeBSD-SA-08:05.openssh

When logging in via SSH with X11-forwarding enabled, sshd(8) fails to correctly handle the case where it fails to bind to an IPv4 port but successfully binds to an IPv6 port. In this case, applications which use X11 will connect to the IPv4 port, even though it had not been bound by sshd(8) and is therefore not being securely forwarded.

### III. Impact

A malicious user could listen for X11 connections on a unused IPv4 port, e.g tcp port 6010. When an unaware user logs in and sets up X11 forwarding the malicious user can capture all X11 data send over the port, potentially disclosing sensitive information or allowing the execution of commands with the privileges of the user using the X11 forwarding.

NOTE WELL: FreeBSD ships with IPv6 enabled by default in the GENERIC and SMP kernels, so users are vulnerable even they have not explicitly enabled IPv6 networking.

### IV. Workaround

Disable support for IPv6 in the sshd(8) daemon by setting the option "AddressFamily inet" in /etc/ssh/sshd\_config.

Disable support for X11 forwarding in the sshd(8) daemon by setting the option "X11Forwarding no" in /etc/ssh/sshd\_config.

### V. Solution

Perform one of the following:

1) Upgrade your vulnerable system to 5-STABLE, 6-STABLE, or 7-STABLE, or to the RELENG\_7\_0, RELENG\_6\_3, RELENG\_6\_2, RELENG\_6\_1, RELENG\_5\_5 security branch dated after the correction date.

2) To patch your present system:

The following patch has been verified to apply to FreeBSD 5.5, 6.1, 6.2, 6.3, and 7.0 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-08:05/openssh.patch  
# fetch http://security.FreeBSD.org/patches/SA-08:05/openssh.patch.asc
```

b) Execute the following commands as root:

```
# cd /usr/src  
# patch < /path/to/patch  
# cd /usr/src/secure/lib/libssh
```

## FreeBSD Security Advisory FreeBSD-SA-08:05.openssh

```
# make obj && make depend && make && make install
# cd /usr/src/secure/usr.sbin/sshd
# make obj && make depend && make && make install
# /etc/rc.d/sshd restart
```

### VI. Correction details

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

Branch Revision  
Path

---

```
RELENG_5
src/crypto/openssh/channels.c 1.18.2.1
RELENG_5_5
src/UPDATING 1.342.2.35.2.21
src/sys/conf/newvers.sh 1.62.2.21.2.22
src/crypto/openssh/channels.c 1.18.8.1
RELENG_6
src/crypto/openssh/channels.c 1.20.2.3
RELENG_6_3
src/UPDATING 1.416.2.37.2.6
src/sys/conf/newvers.sh 1.69.2.15.2.5
src/crypto/openssh/channels.c 1.20.2.2.4.1
RELENG_6_2
src/UPDATING 1.416.2.29.2.16
src/sys/conf/newvers.sh 1.69.2.13.2.15
src/crypto/openssh/channels.c 1.20.2.2.2.1
RELENG_6_1
src/UPDATING 1.416.2.22.2.27
src/sys/conf/newvers.sh 1.69.2.11.2.26
src/crypto/openssh/channels.c 1.20.2.1.4.1
RELENG_7
src/crypto/openssh/channels.c 1.23.2.1
RELENG_7_0
src/UPDATING 1.507.2.3.2.5
src/sys/conf/newvers.sh 1.72.2.5.2.5
src/crypto/openssh/channels.c 1.23.4.1
```

---

### VII. References

<http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=463011>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1483>  
<http://www.openssh.com/txt/release-5.0>

The latest revision of this advisory is available at  
<http://security.FreeBSD.org/advisories/FreeBSD-SA-08:05.openssh.asc>

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

Version: GnuPG v1.4.7 (FreeBSD)

FreeBSD Security Advisory FreeBSD-SA-08:05.openssh

iD8DBQFIBpWTFdaIBMps37IRAomdAJ9hKgp/MG2PbVVojAMjCTtcY6T5HgCeNDxa  
iA55tmcA3GXbsXAd/flJZO4=  
=joYI  
-----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"