-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA512

```
=============================================================================
FreeBSD-SA-16:33.openssh                                    Security Advisory
                                                          The FreeBSD Project

Topic:          OpenSSH Remote Denial of Service vulnerability

Category:       contrib
Module:         OpenSSH
Announced:      2016-11-02
Affects:        All supported versions of FreeBSD.
Corrected:      2016-11-02 06:56:35 UTC (stable/11, 11.0-STABLE)
                2016-11-02 07:23:19 UTC (releng/11.0, 11.0-RELEASE-p3)
                2016-11-02 06:58:47 UTC (stable/10, 10.3-STABLE)
                2016-11-02 07:23:36 UTC (releng/10.3, 10.3-RELEASE-p12)
CVE Name:       CVE-2016-8858

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

During the SSH handshake procedure, the client and server exchanges the
supported encryption, MAC and compression algorithms along with other
information to negotiate algorithms for initial key exchange, with a
message named SSH_MSG_KEXINIT.

II.  Problem Description

When processing the SSH_MSG_KEXINIT message, the server could allocate
up to a few hundreds of megabytes of memory per each connection, before
any authentication take place.

III. Impact

A remote attacker may be able to cause a SSH server to allocate an excessive
amount of memory.  Note that the default MaxStartups setting on FreeBSD will
limit the effectiveness of this attack.

IV.  Workaround

No workaround is available, but systems where sshd(8) is not used are
not vulnerable.

V.   Solution

Perform one of the following:

1) Upgrade your vulnerable system to a supported FreeBSD stable or
release / security branch (releng) dated after the correction date.

The sshd(8) service has to be restarted after the update.  A reboot
is recommended but not required.

2) To update your vulnerable system via a binary patch:

Systems running a RELEASE version of FreeBSD on the i386 or amd64
```

platforms can be updated via the freebsd-update(8) utility:

```
# freebsd-update fetch
# freebsd-update install
```

The sshd(8) service has to be restarted after the update. A reboot
is recommended but not required.

3) To update your vulnerable system via a source code patch:

The following patches have been verified to apply to the applicable
FreeBSD release branches.

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

```
# fetch https://security.FreeBSD.org/patches/SA-16:33/openssh.patch
# fetch https://security.FreeBSD.org/patches/SA-16:33/openssh.patch.asc
# gpg --verify openssh.patch.asc
```

b) Apply the patch. Execute the following commands as root:

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

c) Recompile the operating system using buildworld and installworld as
described in <URL:https://www.FreeBSD.org/handbook/makeworld.html>.

The sshd(8) service has to be restarted after the update. A reboot
is recommended but not required.

VI. Correction details

The following list contains the correction revision numbers for each
affected branch.

Branch/path	Revision
stable/10/	r308199
releng/10.3/	r308203
stable/11/	r308198
releng/11.0/	r308202

To see which files were modified by a particular revision, run the
following command, replacing NNNNNN with the revision number, on a
machine with Subversion installed:

```
# svn diff -cNNNNNN --summarize svn://svn.freebsd.org/base
```

Or visit the following URL, replacing NNNNNN with the revision number:

<URL:https://svnweb.freebsd.org/base?view=revision&revision=NNNNNN>

VII. References

<URL:http://seclists.org/oss-sec/2016/q4/195>

<URL:https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-8858>

The latest revision of this advisory is available at
<URL:https://security.FreeBSD.org/advisories/FreeBSD-SA-16:33.openssh.asc>
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v2.1.15 (FreeBSD)

```
iQIcBAEBCgAGBQJYGZhkAAoJEO1n7NZdz2rnws4P/0i2V2lw3snDi4oVsX2AVkl+
bQ9iRUvgO0SSB4b8JZ8dK6wws8InDR8oihm8jBsaOYPOxu7Wz9Zua2ZAjBAY/GLB
o2+2UMGKVNlP59D/pwBD3qWEjG2KYpE5hItX7iykjwDvd8c7UOLZt7oofVfq8R7D
84BkMQb9DM/1PwFI+ztMYN3uAlzsNxi0GqoHe7PBYmA5rq3QF9LoUlRyOW9KQq8Q
TsBg8briGhy44XifhxU7eUsPUrxJLb5c/w3xsuzSw1AFpgSAc8IKAcrknnTdy+0c
k5GfJz/84xcN1/HO6FDVtYgIoOK2C/ljCHiRAPRsVK3TvXl6agErVBf3CTvWKjg9
NY6QD0KTJw5QF0LT6GbLRAdwnAexQI0U7Hw3Xylv2CFnaxsdYeB9YTVqqMricUqQ
7GZ/ktiXJwBpDLkaieeI6WhbAVdsNQc5A1UWQwjv6mFr5TKhOFWvmHRo/KZprWqd
vFqYNHc3NngcKs537WOXchNnW46hWMsiis/1mJfiRZd89rzq5Dtz7tCcX1c7RgRW
4h0vhtqRMQraby0fI0ND3kC7EnXchMqWAoQ3Tric+2yWQMW/OGDvWXWbM0HqUKq7
7fOGMmXmLhQnkykf4uwjrP4cyMSzSbGdrLQxpwWPwZoH47es/qYKHukBRcnmEkA+
VpT6Vpm0Lqi80W5bh783
=xyal
-----END PGP SIGNATURE-----
```