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

==========
FreeBSD-SA-17:01.openssh Security Advisory
The FreeBSD Project

Topic: OpenSSH multiple vulnerabilities

Category: contrib
Module: OpenSSH
Announced: 2017-01-11
Affects: All supported versions of FreeBSD.
Corrected: 2017-01-11 05:56:40 UTC (stable/11, 11.0-STABLE)
2017-01-11 06:01:23 UTC (releng/11.0, 11.0-RELEASE-p7)
2017-01-11 05:56:40 UTC (stable/10, 10.3-STABLE)
2017-01-11 06:01:23 UTC (releng/10.3, 10.3-RELEASE-p16)
CVE Name: CVE-2016-10009, CVE-2016-10010

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.

OpenSSH supports accessing keys provided by a PKCS#11 token.

II. Problem Description

The ssh-agent(1) agent supports loading a PKCS#11 module from outside a
trusted whitelist. An attacker can request loading of a PKCS#11 module
across forwarded agent-socket. [CVE-2016-10009]

When privilege separation is disabled, forwarded Unix domain sockets
would be created by sshd(8) with the privileges of 'root' instead of
the authenticated user. [CVE-2016-10010]

III. Impact

A remote attacker who have control of a forwarded agent-socket on a
remote system and have the ability to write files on the system
running ssh-agent(1) agent can run arbitrary code under the same user
credential. Because the attacker must already have some control on
both systems, it is relatively hard to exploit this vulnerability in
a practical attack. [CVE-2016-10009]

When privilege separation is disabled (on FreeBSD, privilege separation
is enabled by default and has to be explicitly disabled), an authenticated
attacker can potentially gain root privileges on systems running OpenSSH
server. [CVE-2016-10010]

IV. Workaround

Systems not running ssh-agent(1) and sshd(8) services are not affected.

System administrators may remove ssh-agent(1) to mitigate CVE-2016-10009.

System administrators should enable privilege separation when running
OpenSSH server, which is the FreeBSD default, to mitigate CVE-2016-10010.

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.

Kill all running ssh-agent(1) process and restart sshd(8) service.
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
```

Kill all running ssh-agent(1) process and restart sshd(8) service.
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-17:01/openssh.patch
# fetch https://security.FreeBSD.org/patches/SA-17:01/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>.

Kill all running ssh-agent(1) process and restart sshd(8) service.
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/	r311915
releng/10.3/	r311916
stable/11/	r311915
releng/11.0/	r311916

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:https://www.openssh.com/txt/release-7.4>

<URL:https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-10009>

<URL:https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-10010>

The latest revision of this advisory is available at
<URL:https://security.FreeBSD.org/advisories/FreeBSD-SA-17:01.openssh.asc>
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v2.1.16 (FreeBSD)

iQIzBAEBCgAdFiEEHPf/b631yp++G4yy7Wfs1l3PaucFAlh1yuAACgkQ7Wfs1l3P
auebFA//TGtwrub7JNTgKdc5qnpw+s8W1j0AnQ4wTaJ6v7zNyUB0DG+LHW4uXCwR
xc9Etd2mhY26wJIUxx0Z3oArcqVBGpCGbozuIOU6AdgmHdOL3ddj8aq4SuC0PyMA
0OvNgZIRPZxEm81MP+6/GES4JLmOumiNeAG/MrtITGJDP/K5vVPIst/+F7OJ4P2+
OGrjqBWmAz2EMG62QUJI8oSwB+FJpXtWHKOC4fPGibAQe3vF1WequbcDkLsYl1pX
Ktlk/qh9ivaQreM9rHkUDF0PYwFdsXzveze/TLNbEo+w43v/PAlyR+xw2+22VjGK
fxTL8Gk2tMQfahGZwFmmQFPLcwNRcdjgnZcRRHA3z8vKgM831A53gV3KskUwZl4V
DyKdXtl44zrZ7PtPJ1gJkPK6B8zzfjnSwzPC51pDjh30ps28Rgfc6JOyjxhX5BJ4
sXvQ3meiEfVgVq3DpTqQ3mZVQ1pRF+yhPf1Ptts9fQzAD95JsFF0WT0nzbYoB2VY
KrU4V7d/Ys+HIeQWgDwZlFuLOULlVZDW/H55PT5Tx9JvP5vRlZS/w2HHN7wwy8n5
tNX9mcH8DuG7X/jWDR9ompbJp5uZqcKWVMHPQY7fnaLSJoQMqrpPgZ9tsw6wq347
Vslm3qQwUTSGRagH0rBuHiVJmY/AeqY3lvsaZklWGIYMRjmUeA0=
=3z/p
-----END PGP SIGNATURE-----
```