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

=============================================================================
FreeBSD-SA-16:07.openssh                                  Security Advisory
                                                        The FreeBSD Project

Topic:          OpenSSH client information leak

Category:       contrib
Module:         openssh
Announced:      2016-01-14
Credits:        Qualys Security Advisory Team
Affects:        All supported versions of FreeBSD.
Corrected:      2016-01-14 22:42:43 UTC (stable/10, 10.2-STABLE)
                2016-01-14 22:45:33 UTC (releng/10.2, 10.2-RELEASE-p10)
                2016-01-14 22:47:54 UTC (releng/10.1, 10.1-RELEASE-p27)
                2016-01-14 22:50:35 UTC (stable/9, 9.3-STABLE)
                2016-01-14 22:53:07 UTC (releng/9.3, 9.3-RELEASE-p34)
CVE Name:       CVE-2016-0777

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.  The ssh(1) is client side utility used
to login to remote servers.

II.  Problem Description

The OpenSSH client code contains experimental support for resuming SSH
connections (roaming).  The matching server code has never been shipped, but
the client code was enabled by default and could be tricked by a malicious
server into leaking client memory to the server, including private client
user keys.

III. Impact

A user that authenticates to a malicious or compromised server may reveal
private data, including the private SSH key of the user.

IV.  Workaround

The vulnerable code in the client can be completely disabled by adding
'UseRoaming no' to the global ssh_config(5) file, or to user configuration
in ~/.ssh/config, or by passing -oUseRoaming=no on the command line.

All current remote ssh(1) sessions need to be restared after changing
the configuration file.

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.

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
```

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-16:07/openssh.patch
# fetch https://security.FreeBSD.org/patches/SA-16:07/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>.

VI. Correction details

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

Branch/path	Revision
stable/9/	r294053
releng/9.3/	r294054
stable/10/	r294049
releng/10.1/	r294051
releng/10.2/	r294052

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://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0777>

The latest revision of this advisory is available at <URL:https://security.FreeBSD.org/advisories/FreeBSD-SA-16:07.openssh.asc>

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

iQIcBAEBCgAGBQJWmH8uAAoJEO1n7NZdz2rnZ3MQAMPm2/+gM/83HbibOzRXfo7v
4D3j93BOEGltCQx8y+Stu3Y/CNA6eRYVPvD0u65DeO2bevQcYPQbfHSa5fxYgjWQ
yqmLAvB+KZyGxAWZZhXsOWS6oUsK6y75jaWho3Oq19VLps8CWqHauvIyk0b1z/KA
IlYYcXOdAvDgLoZHVcLbKU0jdOvMmc/iwxhx0aPVu4D2LXIr59xQcA/AsbKobk5V
oqWt5CaaiZCXmVaw9eQhqNuXYC3zoY2/eh8FKG6IkIH9eyL6qQUIxumluxcui1MZ
25tZjp+OsmpVLgWxUyKKyQOVj3rRjaiRBwyUMUk+87GwmW+5b71UYjtVfQw9KHf1
KjGfylhu1oFcw5vCiul9xMm5jtBweqly1U1GEigybkDzaRNM3wheaOjWJVplU9Ku
pNYZJo7cBi19KztUUyF9AUroAdVGVO4fzRtHxWUPIBxXFpgvlXijw/AMckTGcqWy

```
TcEh45zSs2TScP1F8GeLPvmWUFbcChTCYWUIzFVUakEVeM5iRmx6B9qMFcN7YUS7
aFiraTIJFhaYrBbKK95CMfFvDAXwe+tBoGfLjXIfZdHcrmB6jkDyUue8ItopsAS0
hozJQUgcnZzzG+KcWODEB2xMdZSqldUoztDXJII3aisCf39ZXN5IFNJHti13tc8l
Lw/p7lOx/U4SIq+QNqqy
=EApM
-----END PGP SIGNATURE-----
```