Message-Id: <201401291350.s0TDo8hw020342@linus.mitre.org>
Date: Wed, 29 Jan 2014 08:50:08 -0500 (EST)
From: cve-assign@...re.org
To: kseifried@...hat.com
Cc: cve-assign@...re.org, oss-security@...ts.openwall.com
Subject: Re: OpenSSH J-PAKE vulnerability (no cause for panic! remain calm!)

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

Use CVE-2014-1692. The CVE description will indicate that the issue
requires an unusual installation.

> As I understand it this can be enabled via code edit/gcc command line
> options, so not sure if this qualified for a CVE or not (vuln in code,
> yes, is code reachable? not under any default setup, and even on
> non-default you have to go pretty far off to enable it).

An impact on the default installation isn't necessary. Vulnerabilities
that occur only after the user modifies code aren't eligible for a
CVE. However, if there's some type of "installation option" mentioned
by the vendor, someone may have chosen that option, and it may be
worthwhile to track the issue with a CVE. The nature of an
"installation option" obviously varies widely across both open-source
and closed-source products.

In this case, there's:

> http://www.openbsd.org/cgi-bin/cvsweb/src/usr.bin/ssh/Makefile.inc

> Add support for an experimental zero-knowledge password authentication
> method using the J-PAKE protocol ...

> This is experimental, work-in-progress code and is presently
> compiled-time disabled (turn on -DJPAKE in Makefile.inc).

> http://www.openbsd.org/cgi-bin/cvsweb/~checkout~/src/usr.bin/ssh/Makefile.inc?rev=1.41;content-type=text%2Fplain

> #CFLAGS+=   -DJPAKE

This is close to the edge of what "installation option" means, but our
feeling is that the vendor wouldn't have provided that #CFLAGS line at
all unless it were expected that an end user might want to make the
one-character change.

- --
CVE assignment team, MITRE CVE Numbering Authority
M/S M300
202 Burlington Road, Bedford, MA 01730 USA
[PGP key available through http://cve.mitre.org/cve/request_id.html]
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.14 (SunOS)

iQEcBAEBAgAGBQJS6QaDAAoJEKllVAevmvmsKSMIAMCigEPGWSSC3EZgYQvK1o7g
Gs5QBsUAyQBtCZShsSW6rgF4Fu5V/FMOMQLW2Fdjyyq+kY7oubR/TRkOCLcB3TUj
bdTtnbJ6cOHO9q9nLlxg39gjz4zsJeuE6tvZ05sxlpI9RQmVeWnhi6xo7+r4sZ50
T6zg0Im4b+LYOmpK5FwEsWjxoB5kaovWAyLmDqQyDZxGIagq1QPhel/rUMWI+Gds
wXgyOvw+8ARp2nHUaGcxZ3zmlweooneO1SCLfHdU8iVohdtBGOLBYyXy624ty9gf
6y3/wBnzAuzT7ToNc6ijaUlS2tO9Wc0b5QsirxVnOC7Se/0+LH1kT+Fmp4j4XKk=
=Br7x
-----END PGP SIGNATURE-----