Message-ID: <52E877AF.9030205@redhat.com>
Date: Tue, 28 Jan 2014 20:38:23 -0700
From: Kurt Seifried <kseifried@...hat.com>
To: Open Source Security <oss-security@...ts.openwall.com>,
        Assign a CVE Identifier <cve-assign@...re.org>
Subject: OpenSSH J-PAKE vulnerability (no cause for panic! remain calm!)

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

http://www.openbsd.org/cgi-bin/cvsweb/src/usr.bin/ssh/schnorr.c

Revision 1.10: download - view: text, markup, annotated - select for diffs
Wed Jan 29 00:21:41 2014 UTC (3 hours, 14 minutes ago) by djm
Branches: MAIN
CVS tags: HEAD
Diff to: previous 1.9: preferred, coloured
Changes since revision 1.9: +4 -1 lines
In the experimental, never-enabled JPAKE code: clear returned digest and
length in hash_buffer() for error cases; could lead to memory corruption
later if EVP_Digest* fails. Pointed out by Mark Dowd

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).

- --
Kurt Seifried Red Hat Security Response Team (SRT)
PGP: 0x5E267993 A90B F995 7350 148F 66BF 7554 160D 4553 5E26 7993
-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1

iQIcBAEBAgAGBQJS6HevAAoJEBYNRVNeJnmTFcgP/3oYP20fflvJfWw4prATaws3
zZT3MFjmzEy6DJFrAsW9VXNYfUsTKxyf+vI4f1njKUUi7MdYb6HTIbeI/9zu8fP3
zqf3KDLKYZJsO/mC5zm/r+2lduFXNMg8zFkxNci3mNFSwkH0yr4YCaoTlNZlQITY
2dIZDnS0s+vfumd5Epv1+PRGhGxTOfJQIqSw/Li1YAVcIBPgOthN6Wpo2kiwLuJR
/AOkSNDOHTq8//xkQLsnaeOxQMqzo+s/NU5oNX7Me9QWmjnKDipEcUVYcbZ9SyhZ
DcXrxpm9J+iyWCuMgZX8LokscRhmJVi5sJWA4U9xVy/hi0zZYzIQrCXbhEfDM+g3
sKZWUvWrsoMC5mUhqwQyMGRP0o/qTtBN3qz1gNY0jy0zd0Bzi8Fi7++MGyN7H5pv
ymLrpiQvKGC3Pu7SPBPcYDi1jdK+VZ9ztFUTxTvkzn0+LjGxf7+GZuPfrn0CH2em
CeCi4o/CiFI4fKr0cMu10uwBfmGxKKSG+eWjSYySVkvO0xLs9I91Ksby69jTGjAp
6Ln8XtQgSRDJ6hKba6Wox5RxDiuNhitlUD2mcm+5s1SuV+EQzegaX6CTbaO8Zgy5
W7QwDU2M1RcY7VTTDrAg2Grscint106UZmZiiOLsT2R3/cbv7EOISgXTybEdPT3g
bClWQdKuzSxlPrjIp7AT
=dkva
-----END PGP SIGNATURE-----