



Products

Services

Publications

Resources

What's new

Follow @Openwall on Twitter for new release announcements and other news

[<prev] [next>] [thread-next>] [day] [month] [year] [list]

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  
 zZT3MFjnzEy6DJFrAsW9VXNYfUsTKxyf+vI4f1njKUU7MdYb6HTIbeI/9zu8fP3  
 zqf3KDLKYZJs0/mC5zm/r+2lduFXNMg8zFkxNci3mNFSwkH0yr4YCaoTlNZlQITY  
 2dIZDnS0s+vfumd5Epl+PRGhGxTofJQIqSw/Li1YAVcIBPg0thN6Wpo2kiwLuJR  
 /A0kSND0HTq8//xkQLsnae0xQMqzo+s/NU5oNX7Me9QWmjnKDipEcUVYcbZ9SyhZ  
 DcXrxpm9J+iyWCuMgZX8LokscRhmJVi5sJWA4U9xVy/hi0zZYzIQRcXbhEfDM+g3  
 sKZUvWrs0MC5mUhwQyMGRP0o/qTtBN3qz1gNY0jy0zd0Bzi8Fi7++MGyN7H5pv  
 ymLrpiQvKGC3Pu7SPBPCyDi1jdK+VZ9ztFUTxTvkn0+LjGxf7+GZuPfrn0CH2em  
 CeCi4o/CiFI4fKr0cMu10uwBfmGxKKSG+eWjSYySVkv00xLs9I91Ksby69jTGjAp  
 6Ln8XtQgSRDJ6hKba6Wox5RxDiunhitlUD2mcm+5s1SuV+EQzegaX6CTba08Zgy5  
 W7QwDU2M1RcY7VTTDrAg2Grscint106UZmZii0LsT2R3/cbv7E0ISgXTybEdPT3g  
 bClWQdKuzSxlPrjIp7AT  
 =dkva  
 -----END PGP SIGNATURE-----

Powered by blists - [more mailing lists](#)

Please check out the [Open Source Software Security Wiki](#), which is counterpart to this [mailing list](#).

Confused about [mailing lists](#) and their use? [Read about mailing lists on Wikipedia](#) and check out these [guidelines on proper formatting of your messages](#).