Exploit Fully Breaks SHA-1, Lowers the Attack Bar

Published by Slashdot *on 24 Jan 2020*

ThreatPost reported on some big research last week:A proof-of-concept attack has been pioneered that "fully and practically" breaks the Secure Hash Algorithm 1 (SHA-1) code-signing encryption, used by legacy computers to sign the certificates that authenticate software downloads and prevent man-in-the-middle tampering. The exploit was developed by Gatan Leurent and Thomas Peyrin, academic researchers at Inria France and Nanyang Technological University/Temasek Laboratories in Singapore. They noted that because the attack is much less complex and cheaper than previous PoCs, it places such attacks within the reach of ordinary attackers with ordinary resources. "This work shows once and for all that SHA-1 should not be used in any security protocol where some kind of collision resistance is to be expected from the hash function," the researchers wrote. "Continued usage of SHA-1 for certificates or for authentication of handshake messages in TLS or SSH is dangerous, and there is a concrete risk of abuse by a well-motivated adversary. SHA-1 has been broken since 2004, but it is still used in many security systems; we strongly advise users to remove SHA-1 support to avoid downgrade attacks." Given the footprint of SHA-1, Leurent and Peyrin said that users of GnuPG, OpenSSL and Git could be in immediate danger. Long-time Slashdot reader shanen writes, "I guess the main lesson is that you can never be too sure how long any form of security will remain secure."Read more of this story at Slashdot.

Click here to read full news..