The researchers successfully cracked 1024-bit RSA in GnuPG Crypto Library

Security researchers have discovered an important flaw in the GnuPG cryptographic library that completely disables 1024-bit RSA and successfully retrieves the RSA secret key to decrypt the data.

Security researchers have discovered an important flaw in the GnuPG cryptographic library that completely disables 1024-bit RSA and successfully retrieves the RSA secret key to decrypt the data.

More information: RSA is a public key data encryption algorithm, the longer the RSA key, the greater the security level, and therefore, it is commonly used in e-commerce with a key length of sufficiently large. . RSA with the higher number of bits, the more time and effort it takes to break it. 256-bit keys can easily be broken in a few hours, 512-bits will require several hundred computers to work at the same time to analyze. Therefore, 1024-bit will take more time, but recently it has started to appear problems and can be cracked in a few hours. 2048-bit is currently recommended by security researchers, because it is more secure. If you can create a 4096-bit key, it is completely reassuring, because it is almost impossible to crack in the near future.

Gnu Privacy Guard (GnuPG or GPG) is open source software that is popular with many operating systems from Linux, FreeBSD to Windows and macOS X. It is quite similar to the software used by the NSA (National Security Agency). United States) and Edward Snowden to keep their communications safe from law enforcement.

The vulnerability, named CVE-2017-7526, is located in the Libgcrypt encoding library used by GnuPG, vulnerable to the FLUSH + RELOAD side-channel attack.

A group of researchers from Eindhoven Technical University, University of Illinois, University of Pennsylvania, University of Maryland, and University of Adelaide - discovered that the "left-to-right window" method is used

by letters. Libgcrypt institute to provide encryption algorithm, leaked significant information about the number of bits of the exponent, more from right to left, allowing full RSA key recovery. Specifically the information of model squarings and multiplications in left-to-right sliding window revealed can use the Heninger-Shacham extension algorithm to restore part of the secret key, thereby completely recovering the secret key for RSA-1024.

"In this article, we have demonstrated the complete unlocking of RSA-1024 as done in Libgcrypt. Assuming Libgcrypt uses the method from left to right to calculate the sliding-window expansion. "researchers wrote in the research paper.

L3 Cache Side-Channel Attack requires hackers to run arbitrary software on the hardware that the secret RSA key is used. This type of attack allows a hacker to obtain a secret decryption key from the system by analyzing the memory usage model or the device's electromagnetic outputs generated during the decoding process.

"Although in fact, there are more easy ways to get secret keys than Side-Channel Attack, but in the case of using a virtual machine, this type of attack can be used by a virtual machine to steal. secret keys from another virtual machine ", Libgcrypt advises.

The researchers also said that this Side-Channel Attack attack also works with RSA 2048-bit, which has much greater computational and complexity requirements than 1024-bit RSA.

The article is titled: "Sliding right into disaster: Left-to-right sliding windows leak", written by Daniel J. Bernstein, Joachim Breitner, Daniel Genkin, Leon Groot Bruinderink, Nadia Heninger, Christine van Vredendaal, Tanja Lange and Yuval Yarom.

Libgcrypt has released patch fixes for Libgcrypt version 1.7.8. Debian and Ubuntu have updated their libraries with the latest version of Libgcrypt.

Therefore, you should check if your Linux distribution is running the latest version of the Libgcrypt library.