The Hacker News™
Security in a serious way

Researchers Crack 1024-bit RSA Encryption in GnuPG Crypto Library

Monday, July 03, 2017 Mohit Kumar

Security boffins have discovered a critical vulnerability in a GnuPG cryptographic library that allowed the researchers to completely break RSA-1024 and successfully extract the secret RSA key to decrypt data.

Gnu Privacy Guard (GnuPG or GPG) is popular open source encryption software used by many operating systems from Linux and FreeBSD to Windows and macOS X.

It's the same software used by the former NSA contractor and whistleblower Edward Snowden to keep his communication secure from law enforcement.

The vulnerability, labeled CVE-2017-7526, resides in the **Libgcrypt** cryptographic library used by GnuPG, which is prone to local FLUSH+RELOAD side-channel attack.

A team of researchers — from Technical University of Eindhoven, the University of Illinois, the University of Pennsylvania, the University of Maryland, and the University of Adelaide — found that the "left-to-right sliding window" method used by the libgcrypt library for carrying out the mathematics of cryptography leaks significantly more information about exponent bits than for right-to-left, allowing full RSA key recovery.

> "In this paper, we demonstrate a complete break of RSA-1024 as implemented in Libgcrypt. Our attack makes essential use of the fact that Libgcrypt uses the left-to-right method for computing the sliding-window expansion," the researchers wrote in the research paper.

> "The pattern of squarings and multiplications in left-to-right sliding windows leaks significantly more information about the exponent than right-to-left. We show how to extend the Heninger-Shacham algorithm for partial key reconstruction to make use of this information and obtain a very efficient full key recovery for RSA-1024."

L3 Cache Side-Channel Attack requires an attacker to run arbitrary software on the hardware where the private RSA key is used.

The attack allows an attacker to extract the secret crypto key from a system by analyzing the pattern of memory utilization or the electromagnetic outputs of the device that are emitted during the decryption process.

> "Thus in practice, there are easier ways to access the private keys than to mount this side-channel attack. However, on boxes with virtual machines, this attack may be used by one VM to steal private keys from another VM," Libgcrypt advisory reads.

Researchers have also provided evidence that the same side channel attack also works against RSA-2048, which require moderately more computation than RSA-1024.

The research paper titled, 'Sliding right into disaster: Left-to-right sliding windows leak,' was authored by Daniel J. Bernstein, Joachim Breitner, Daniel Genkin, Leon Groot Bruinderink, Nadia Heninger, Christine van Vredendaal, Tanja Lange and Yuval Yarom.

Libgcrypt has released a fix for the issue in Libgcrypt version 1.7.8. Debian and Ubuntu have already updated their library with the latest version of Libgcrypt.

So, you are strongly advised to check if your Linux distribution is running the latest version of the Libgcrypt library.

Mohit Kumar

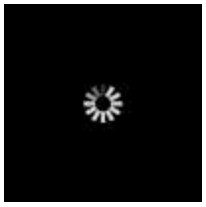
Entrepreneur, Hacker, Speaker, Founder and CEO — The Hacker News and The Hackers Conference.

Cryptographic Library, Cryptography, Encryption, GnuPG, GnuPG Email Encryption, GPG, Hacking News, Libgcrypt, Rsa Encryption, RSA Security, Vulnerability

POPULAR STORIES

Three Hackers Plead Guilty to Creating IoT-based Mirai DDoS Botnet

Pre-Installed Password Manager On Windows 10 Lets Hackers Steal All Your Passwords



FCC Just Killed Net Neutrality—What Does This Mean? What Next?

Learn Ethical Hacking Online: A to Z Training Courses

TRITON Malware Targeting Critical Infrastructure Could Cause Physical Damage

This New Android Malware Can Physically Damage Your Phone

Collection of 1.4 Billion Plain-Text Leaked Passwords Found Circulating Online

Firewall Bursting: A New Approach to Better Branch Security

Zero-Day Remote 'Root' Exploit Disclosed In AT&T DirecTV WVB Devices

Password Stealing Apps With Over A Million Downloads Found On Google Play Store