Infineon says has fixed encryption flaw found by researchers

#TECHNOLOGY NEWS

OCTOBER 16, 2017 / 7:28 PM / A MONTH AGO

https://www.reuters.com/article/us-infineon-cyber/infineon-says-has-fixed-encryption-flaw-found-by-researchers-idUSKBN1CL2KC

Douglas Busvine
3 MIN READ

FRANKFURT (Reuters) - Germany's Infineon Technologies said it was aware of, and had taken action to correct a flaw in the encryption used for secure products such as identity cards that was revealed by researchers on Monday.

The vulnerability exposes smartcards, security tokens and other secure hardware chips made by Infineon to a so-called "factorization" attack, the Center for Research on Cryptography and Security said.

It would be feasible for a hacker to compute the private part of an encryption "key" using only the key's public part, the researchers, led by Petr Svenda of the Masaryk University in the Czech Republic, found. (here) Infineon, which makes chips used in the auto industry, power management and smartcard systems, said the researchers had informed the company of the flaw in February.

“Infineon thoroughly investigated the newly developed methods and reacted immediately,” a company spokesman said.

The flaw left 750,000 digital identity cards issued by Estonia vulnerable to attack, the government of the east European country that has been a pioneer of e-government said last month.

On Monday the Estonian authorities said they were taking preventative measures to prevent the exploitation of the possible vulnerability.

Microsoft Corp included an update of the firmware that runs on Infineon’s so-called Trusted Platform Modules to address the security flaw in a release of “patches”, or software fixes, rolled out on Oct. 10.

The flaw resided in the crypto-library used by Infineon, within an algorithm that is used to generate large prime numbers which are then paired.

Infineon used a simplified system for generating these prime numbers called “Fast Prime” that had been officially certified. No mathematical weaknesses were found during the certification process, the company said.

Under a worst-case scenario, however, it would cost just $76 for a hacker to crack a 1024-bit encryption key and about $40,000 for a 2048-bit key using the C4 version of the Amazon Web Services cloud computing platform, the researchers reckon.

“In close cooperation with the research team, our customers and the German certification body, the software function has been updated,” the Infineon spokesman said.

"(It) is currently in the process of being certified and rolled out, including the production of new software devices that use the new software function." The company was not aware of the flaw being successfully exploited by hackers.

Additional reporting by Jim Finkle; Editing by Greg Mahlich
Our Standards:The Thomson Reuters Trust Principles.