Finnish firm detects new Intel security flaw

January 12 2018

A newly-discovered flaw lets assailants take control of a laptop in seconds, an industry firm says

A new security flaw has been found in Intel hardware which could enable hackers to access corporate laptops remotely, Finnish cybersecurity specialist F-Secure said on Friday.

F-Secure said in a statement that the flaw had nothing to do with the "Spectre" and "Meltdown" vulnerabilities recently found in the micro-chips that are used in almost all computers, tablets and smartphones today.

Rather, it was an issue within Intel Active Management Technology (AMT), "which is commonly found in most corporate laptops, (and) allows an attacker to take complete control over a user's device in a matter of seconds," the cybersecurity firm said.

"The issue potentially affects millions of laptops globally."

The flaw was of "an almost shocking simplicity, but its destructive potential is unbelievable," said F-Secure consultant Harry Sintonen, who discovered it.

"In practice, this flaw could give a hacker complete control over the affected laptop, despite the best security measures."

An attacker would initially need physical access to the device in question.

But once they had re-configured AMT, they could effectively "backdoor" the machine and then access the device remotely, by connecting to the same wireless or wired network as the user, F-Secure said.

In certain cases, the assailant could also programme AMT to connect to their own server, which would eliminate the need to be in the same network segment as the victim.

"No other security measures—full disk encryption, local firewall, anti-malware software or VPN—are able to prevent exploitation of this issue."

A successful attack would lead to complete loss of confidentiality, integrity and availability, F-Secure said.

The assailant would be able to read and modify all of the data and applications a user may have access to on their computer. And they could also install malware on the device, even at the firmware level.

F-Secure expert Sintonen said that organizations needed set a strong AMT password or perhaps disable AMT completely if possible.

The recent discovery of the "Spectre" and "Meltdown" vulnerabilities in computer chips made by Intel, AMD and ARM, have sent big names in the sector—including Amazon, Google, Microsoft and Mozilla—rushing out updates and patches to eliminate the flaw.

Citation: Finnish firm detects new Intel security flaw (2018, January 12) retrieved 24 April 2024 from https://phys.org/news/2018-01-finnish-firm-intel-flaw.html