AMD says patches on the way for flawed chips

21 March 2018

AMD expressed confidence that chip vulnerabilities made public last week by Israeli-based security firm CTS Labs could be fixed with firmware patches and updated software that would not slow computers down

Advanced Micro Devices on Tuesday said patches are on the way for recently revealed flaws in some of its chips that could allow hackers to take over computers.

AMD expressed confidence that chip vulnerabilities made public last week by Israeli-based security firm CTS Labs could be fixed with firmware patches and updated software that would not slow computers down.

The chip manufacturer downplayed the threat of hackers taking advantage of the flaws, saying it would require administrator-level access to computers.

"Any attacker gaining unauthorized administrative access would have a wide range of attacks at their disposal well beyond the exploits identified in this research," AMD said in its first update on the situation since the flaws were made public.

CTS Labs published its research showing "multiple critical security vulnerabilities and exploitable manufacturer backdoors" in AMD chips.

The security firm itemized 13 flaws, saying they "have the potential to put organizations at significantly increased risk of cyberattacks."

The report came weeks after Intel disclosed similar hardware-based flaws dubbed Meltdown and Spectre, sparking widespread computer security concerns and a congressional inquiry.

In a 20-page white paper, CTS researchers said the AMD Secure Processor, the gatekeeper responsible for the security of AMD processors, contains "critical vulnerabilities" that "could allow malicious actors to permanently install malicious code inside the Secure Processor itself."

"The vulnerabilities we have discovered allow bad actors who infiltrated the network to persist in it, surviving computer reboots and reinstallations of the operating system," the report said.

"This allows attackers to engage in persistent, virtually undetectable espionage, buried deep in the system."

California-based AMD is one of the largest semiconductor firms specializing in processors for PCs and servers.

"AMD has rapidly completed its assessment and is in the process of developing and staging the deployment of mitigations," the chipmaker said.

"We believe that each of the issues cited can be mitigated through firmware patches and a standard BIOS update, which we plan to release in the coming weeks."