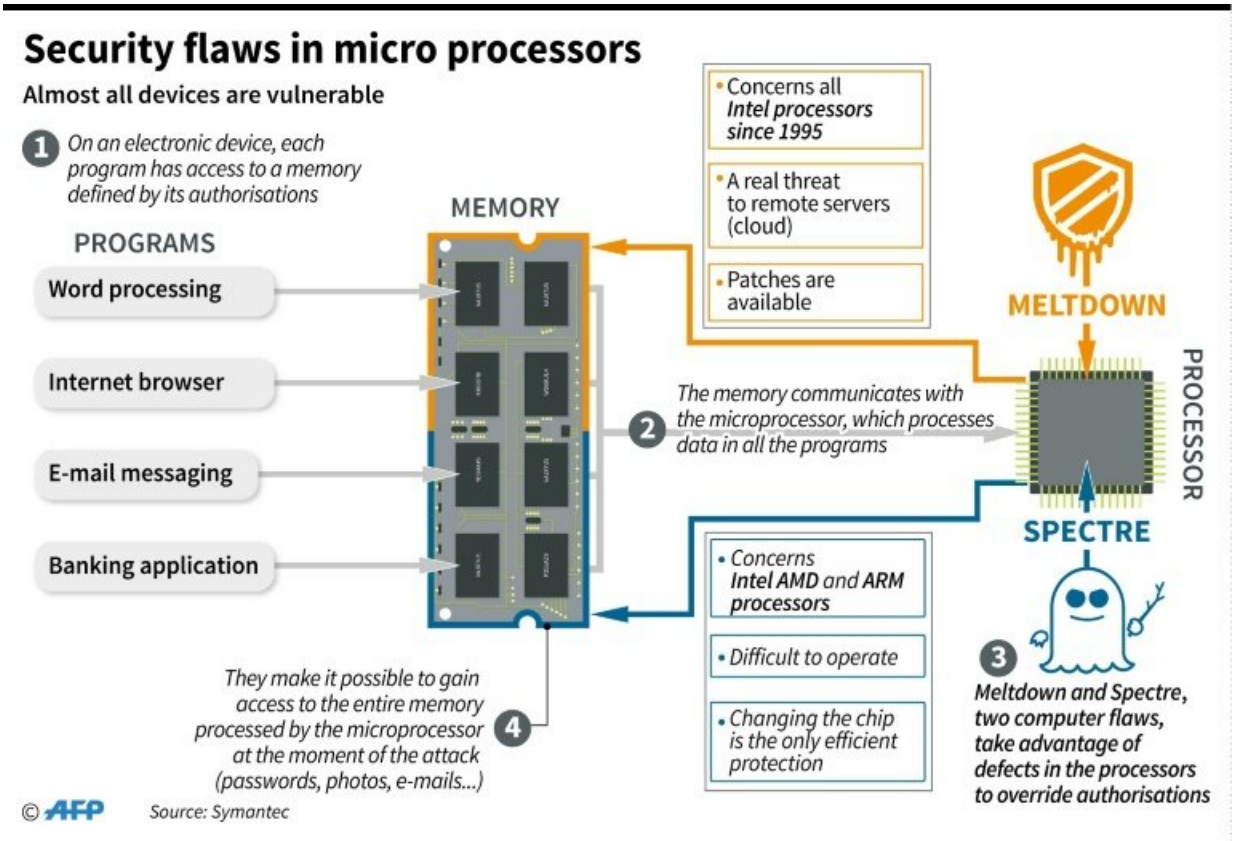
# Researchers find 'critical' security flaws in AMD chips

March 13 2018




Flaws in micro processors

Security researchers said Tuesday they discovered flaws in chips made by Advanced Micro Devices that could allow hackers to take over computers and networks.

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

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

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

CTS said the newly discovered flaws could compromise AMD's new chips that handle applications in the enterprise, industrial and aerospace sectors, as well as consumer products.

In a 20-page white paper, the 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."

"These vulnerabilities could expose AMD customers to industrial espionage that is virtually undetectable by most security solutions," the researchers said.

CTS said AMD's Ryzen chipset, which AMD outsourced to a Taiwanese chip manufacturer, ASMedia, "is currently being shipped with exploitable manufacturer backdoors inside."

This could allow attackers "to inject malicious code into the chip" and create "an ideal target" for hackers, the researchers said.

"CTS believes that networks that contain AMD computers are at a

considerable risk," the report said.

"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.

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

AMD, one of the largest semiconductor firms specializing in processors for PCs and servers, said it was studying the latest report.

"At AMD, security is a top priority and we are continually working to ensure the safety of our users as new risks arise," the California-based company said in a statement.

"We are investigating this report, which we just received, to understand the methodology and merit of the findings."

Analysts at the security firm enSilo said the AMD flaws could be worse than those affecting Intel chips.

"The impact of these vulnerabilities is more severe than Meltdown/Spectre as it allows an attacker to execute highly privileged code and persist on the victim machine," enSilo said in a blog post.

Additionally, some of the flaws may be nearly impossible to patch.

"We estimate that without patches from AMD, protection against the vulnerabilities can be limited at best," enSilo researchers said. "The best protection is to block malware that attempts to leverage these vulnerabilities."