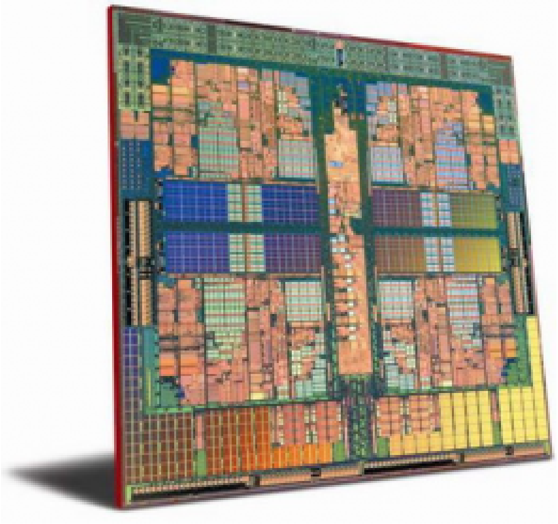
PHYS.ORG

Computer chip 'flaw' sparks security debate amid scramble for fix

January 4 2018



A newly discovered vulnerability in computer chips raised concerns Wednesday that hackers could access sensitive data on most modern systems, as technology firms sought to play down the security risks.

Chip giant Intel issued a statement responding to a flurry of warnings surfacing after researchers discovered the security hole which could allow privately stored data in computers and networks to be leaked.

Intel labeled as incorrect reports describing a "bug" or "flaw" unique to its products.

Intel chief executive Brian Krzanich told CNBC that "basically all modern processers across all applications" use this process known as "access memory," which was discovered by researchers at Google and kept confidential as companies work on remedies.

Google, meanwhile, released findings from its security researchers who sparked the concerns, saying it made the results public days ahead of schedule because much of the information had been in the media.

The security team found "serious security flaws" in devices powered by Intel, AMD and ARM chips and the operating systems running them and noted that, if exploited, "an unauthorized party may read sensitive information in the system's memory such as passwords, encryption keys, or sensitive information open in applications."

"As soon as we learned of this new class of attack, our security and product development teams mobilized to defend Google's systems and our users' data," Google said in a security blog.

"We have updated our systems and affected products to protect against this new type of attack. We also collaborated with hardware and software manufacturers across the industry to help protect their users and the broader web."

Spectre and Meltdown

The Google team said the vulnerabilities, labeled "Spectre" and "Meltdown," affected a number of chips from Intel as well as some from AMD and ARM, which specializes in processors for mobile devices.

Intel said it was working with AMD and ARM Holdings and with the makers of computer operating software "to develop an industry-wide approach to resolve this issue promptly and constructively."

Jack Gold, an independent technology analyst, said he was briefed in a conference call with Intel, AMD and ARM on the issue and that the three companies suggested concerns were overblown.

"All the chips are designed that way," Gold said.

The companies were working on remedies after "some researchers found a way to use existing architecture and get into protected areas of computer memory and read some of the data," he added.

Microsoft said in a statement it had no information suggesting any compromised data but was "releasing security updates today to protect Windows customers against vulnerabilities."

But an AMD spokesman said that because of the differences in AMD processor architecture, "we believe there is near zero risk to AMD products at this time."

ARM meanwhile said it was "working together with Intel and AMD" to address potential issues "in certain high-end processors, including some of our Cortex-A processors."

"We have informed our silicon partners and are encouraging them to implement the software mitigations developed if their chips are impacted," the SoftBank-owned firm said.

Slowdown?

Earlier this week, some researchers said any fix—which would need to be handled by software—could slow down computer systems, possibly by 30 percent or more.

Intel's statement said these concerns, too, were exaggerated.

"Contrary to some reports, any performance impacts are workload-dependent, and, for the average computer user, should not be significant and will be mitigated over time," the company statement said.

Tatu Ylonen, security researcher at SSH Communications Security, said the patches "will be effective" but it will be critical to get all networks and cloud services upgraded, Ylonen said.

British security researcher Graham Cluley also expressed concern "that attackers could exploit the flaw on vulnerable systems to gain access to parts of the computer's memory which may be storing sensitive information. Think passwords, private keys, credit card data."

But he said in a blog post that it was "good news" that the problem had been kept under wraps to allow operating systems such as those from Microsoft and Apple to make security updates before the flaw is maliciously exploited.

Citation: Computer chip 'flaw' sparks security debate amid scramble for fix (2018, January 4) retrieved 27 April 2024 from https://phys.org/news/2018-01-google-flaws-intel-chips.html