New security flaw in Intel chips could affect millions

14 May 2019

In this Oct. 3, 2018, file photo the Intel logo appears on a screen at the Nasdaq MarketSite, in New York's Times Square. Intel has revealed another hardware security flaw that could affects millions of machines around the world. The chipmaker said Tuesday, May 14, 2019, that there's no evidence of bad actors exploiting the bug, which is embedded in the architecture of computer hardware. (AP Photo/Richard Drew, File)

Intel has revealed another hardware security flaw that could affects millions of machines around the world.

The bug is embedded in the architecture of computer hardware, and it can't be fully fixed.

"With a large enough data sample, time or control of the target system's behavior," the flaw could enable attackers to see data thought to be off-limits, Bryan Jorgensen, Intel's senior director of product assurance and security, said in a video statement.

But Intel said Tuesday there's no evidence of anyone exploiting it outside of a research laboratory. "Doing so successfully in the real world is a complex undertaking," Jorgensen said.

It's the latest revelation of a hard-to-fix vulnerability affecting processors that undergird smartphones and personal computers. Two bugs nicknamed Spectre and Meltdown set a panic in the tech industry last year.

Intel said it's already addressed the problem in its newest chips after working for months with business partners and independent researchers. It's also released code updates to mitigate the risk in older chips, though it can't be eliminated entirely without switching to newer chips.

Major tech companies Google, Apple, Amazon and Microsoft all released advisories Tuesday to instruct users of their devices and software, many of which rely on Intel hardware, on how to mitigate the vulnerabilities.

As companies and individual citizens increasingly sign their digital lives over to "the cloud"—an industry term for banks of servers in remote data centers—the digital gates and drawbridges keeping millions of people's data safe have come under increasing scrutiny.

In many cases, those barriers are located at the level of central processing unit, or CPU—hardware that has traditionally seen little attention from hackers. But last year the processor industry was shaken by news that Spectre and Meltdown could theoretically enable hackers to leapfrog those hardware barriers and steal some of the most securely held data on the computers involved.

Although security experts have debated the seriousness of the flaws, they are onerous and expensive to patch, and new vulnerabilities are discovered regularly.

Bogdan Botezatu, director of threat research for security firm Bitdefender, said the latest attack was another reason to question how safe users can really be in the cloud.

"This is a very, very serious type of attack," Botezatu said. "This makes me personally very, very skeptical about these hardware barriers set in place by CPU vendors."

Intel said it discovered the flaw on its own, but credited Bitdefender, several other security firms and academic researchers for notifying the company about the problem.

Botezatu said Bitdefender found the flaw because its researchers were increasingly focused on the safety and management of virtual machines, the term for one or more emulated mini-computers that can be spun up inside a larger machine—a key feature of cloud computing.

More information: zombieloadattack.com/

APA citation: New security flaw in Intel chips could affect millions (2019, May 14) retrieved 23 May 2019 from https://techxplore.com/news/2019-05-flaw-intel-chips-affect-millions.html