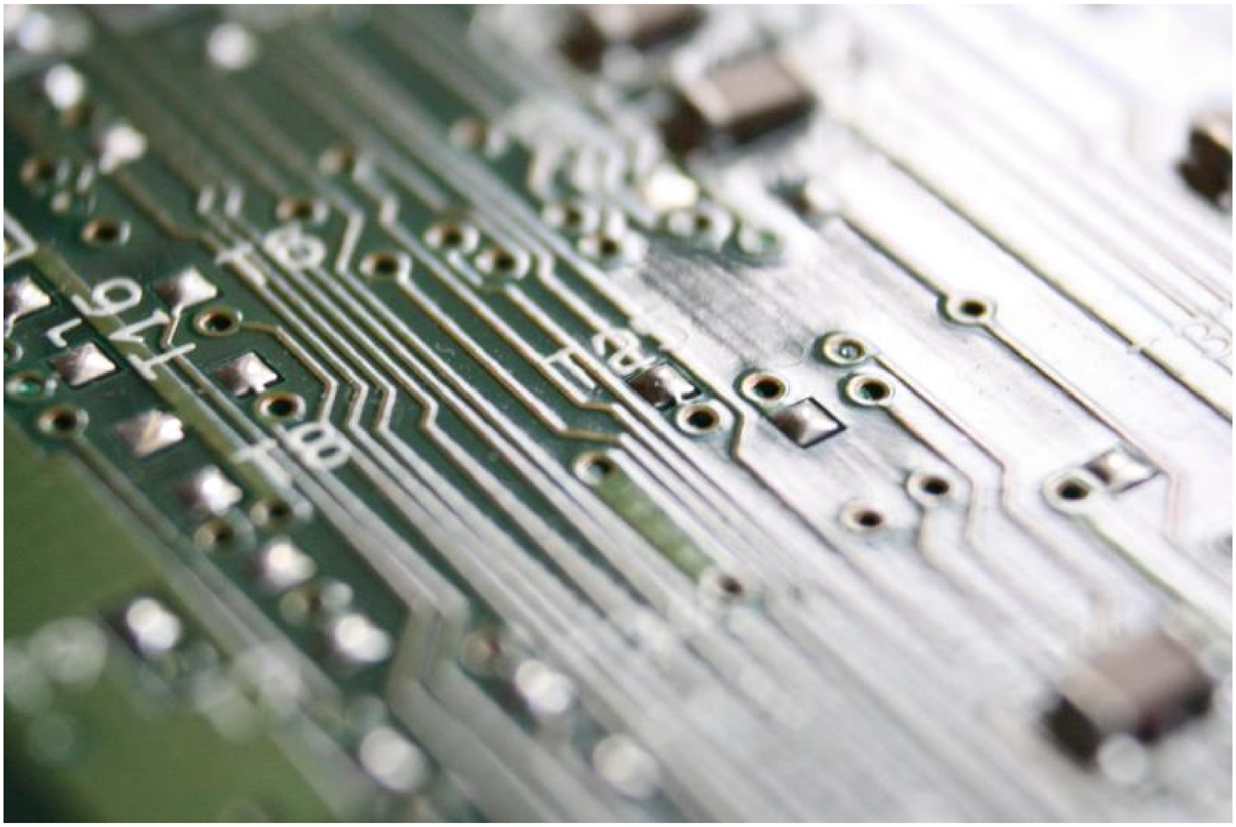
PHYS.ORG

Tech firms rush out patches for 'pervasive' computer flaw

January 5 2018



Credit: Public Domain

Amid a frantic rush to patch a computer security flaw, experts struggled Thursday to determine the impact of a newly discovered vulnerability which could affect billions of devices worldwide.

Cybersecurity researchers called for computer systems to urgently install updates a day after the release of details of the so-called Spectre and Meltdown vulnerabilities affecting the chips powering most modern PCs and many mobile devices.

Researchers on Wednesday published details of the flaw, which unlike many other vulnerabilities stems from the chip itself and how it safeguards private data stored on computers and networks.

The researchers at Google showed how a hacker could exploit the flaw to get passwords, encryption codes and more, even though there have been no reports of any attacks using the vulnerability.

"The full extent of this class of attack is still under investigation and we are working with security researchers and other browser vendors to fully understand the threat and fixes," said Mozilla researcher Luke Wagner in a blog post.

The revelations "attack the foundational modern computer building block capability that enforces protection of the (operating system)," said Steve Grobman, chief technology officer at security firm McAfee.

"Businesses and consumers should update operating systems and apply patches as soon as they become available."

Intel updates

Computer chipmaking giant Intel—the focus of the first reports on the flaw—said the company and its partners "have made significant progress in deploying updates" to mitigate any threats.

"Intel expects to have issued updates for more than 90 percent of processor products introduced within the past five years," an Intel statement said.

"In addition, many operating system vendors, public cloud service providers, device manufacturers and others have indicated that they have already updated their products and services."

But John Bambenek, a Fidelis security researcher who works with the SANS Internet Storm Center, warned that it may be too soon to know the extent of the problem.

"This bug is probably worth its name and logo considering the pervasive nature of the vulnerability," Bambenek said in a blog post.

"Contrary to some initial reporting, this is NOT just an Intel bug, it affects AMD and ARM processors as well. These could even be used in cloud... environments to leak memory outside the running virtual machine."

In a web page dedicated to the vulnerability, security researchers said Meltdown and Spectre may "get hold of secrets stored in the memory of other running programs. This might include your passwords stored in a password manager or browser, your personal photos, emails, instant messages and even business-critical documents."

The two flaws "work on personal computers, mobile devices, and in the cloud," the researchers said.

"All Mac systems and iOS devices are affected, but there are no known exploits impacting customers at this time," Apple said in a post at an online support page

It advised only getting apps from its online App Store which vets programs for safety, and said it has already released some "mitigations" to protect against the exploit and planned to release a defensive update for Safari on macOS and iOS in the coming days.

Some experts pointed out that the only real "fix" in some cases would be replacing the chip itself, which would be a massive issue for the computing industry.

"The good news is patches are out for almost everything," Bambenek said.

"The bad news is, Spectre, in particular can't be completely mitigated by patching as it seems it will require a hardware fix. The good news is that Spectre is harder to exploit."

The US government's Computer Emergency Response Team initially indicated in a bulletin that only a hardware fix would solve the problem, but then removed that from an update.

"Fully removing the vulnerability requires replacing vulnerable CPU (central processing unit) hardware," said the first bulletin.

Citation: Tech firms rush out patches for 'pervasive' computer flaw (2018, January 5) retrieved 10 April 2024 from https://phys.org/news/2018-01-tech-firms-patches-pervasive-flaw.html