Tech firms battle to resolve major security flaw (Update)

January 5 2018

Amazon, Google and now Apple—as the list of digital giants hit by the "Spectre" and "Meltdown" computer security flaws grows longer, the race is on to limit the damage.

"All Mac systems and iOS devices are affected, but there are no known exploits impacting customers at this time," Apple—whose devices are usually regarded as secure—said in a post on an online support page on Thursday.

Almost all microprocessors produced over the past 10 years by Intel, AMD and ARM are affected. No PC or mobile device can function without the miniature components that are effectively nerve centers for executing computer programs and apps.

And that is what distinguishes them from previous security alerts that have tended to involve software rather than hardware.

In theory, Spectre and Meltdown could enable a user to "access kernel level memory access, exposing critical information that would be stored there, like system passwords," said Chris Morales, head of security analytics at Vectra.

Luke Wagner, a software engineer at Mozilla, wrote on a security blog that it was "possible to use similar techniques from web content to read private information".

Effectively, all electronic devices manufactured all around the world in recent years contain potentially vulnerable chips.

The biggest names in the sector, including Amazon, Google, Microsoft and Mozilla, are now rushing out updates and patches to eliminate the flaw.

US giant Intel, as well as its rivals AMD and ARM, have started installing updates.

In a statement on Thursday, Intel said it 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.

Difficult to exploit?

"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."

Apple, for its part, 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.

But some experts believe that the only real "fix" in some cases would be replacing the chip itself, which would be a huge issue for the computing industry.

That said, the experts concede that hacking the chips would require a

very high level of technical expertise and the risks were therefore limited.

The US Computer Emergency Readiness Team (CERT) said that it was "not aware of any active exploitation at this time."

In Germany, the BSI Federal Office for Information Security, similarly found no evidence of any "active exploitation" of the flaw.

In addition to the security flaw, Intel found itself in hot water Friday over the announcement that its chief executive had sold some of his shares in the company.

According to the specialist magazine Solutions Numeriques, Intel was aware of the existence of the security flaw in its chips at the end of November. But in the fourth quarter of last year, CEO Brian Krzanich sold nearly 900,000 shares, halving his stake in the company, according to Bloomberg.

A company spokesman told Bloomberg that the sale had nothing to do with the issue of the security flaw, insisting that Krzanich had exercised options according to a pre-set timetable agreed long before.

Intel shares which slid this week on the news regained slightly less than a percent on Friday to $44.74 at the close of the Nasdaq exchange.

Meanwhile, lawsuits seeking class action status have been filed against Intel in federal courts in three US states.

The civil suits accuse Intel of "unjust and deceptive" tactics that resulted in people buying computers with flawed chips.

A suit filed in federal court in California argued that people with

computers powered by Intel chips are faced with the "unappealing choice" of either replacing the machines or accepting "massive security vulnerabilities" and downgraded performance, the suit argued.