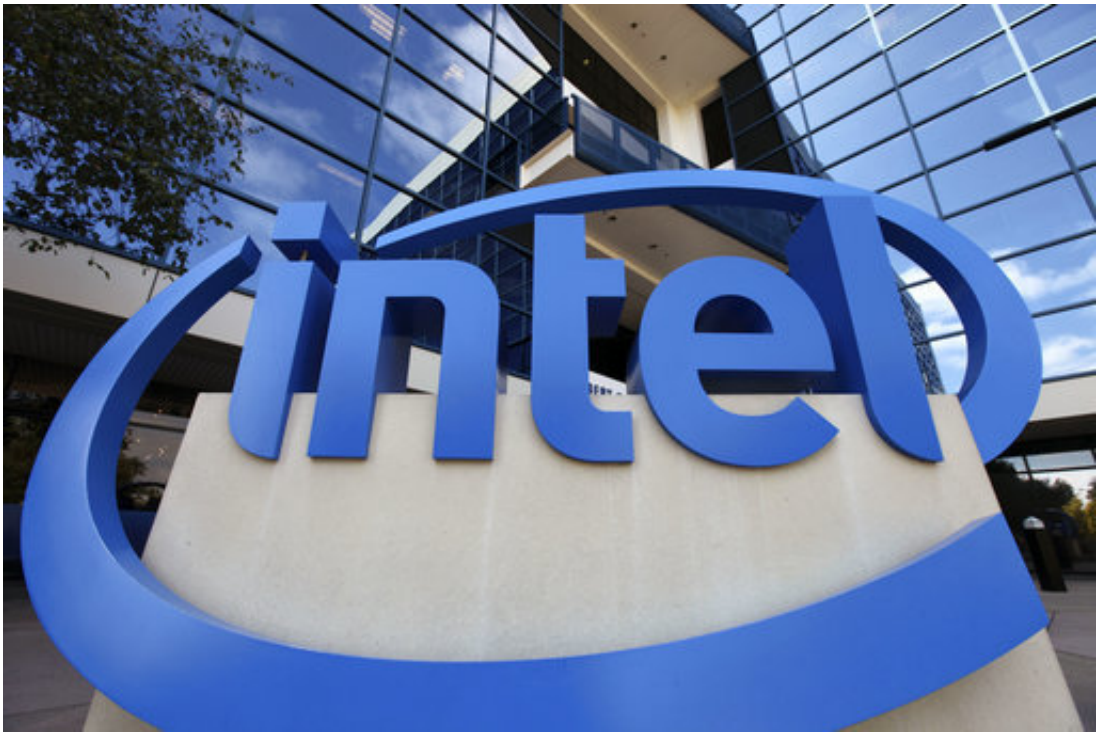
Explainer: Who's affected by computer chip security flaw

January 4 2018, by Matt O'brien



In this July 20, 2011 file photo, Intel corporate offices are seen in Santa Clara, Calif. Intel says it's working to patch a security vulnerability in its products but says the average computer user won't experience significant slowdowns as the problem is fixed. The chipmaker released a statement Wednesday, Jan. 3, 2018, after a report by British technology site The Register caused Intel stocks to trade lower.(AP Photo/Ben Margot)

Technology companies are scrambling to fix serious security flaws

affecting computer processors built by Intel and other chipmakers and found in many of the world's personal computers and smartphones.

The two hardware bugs discovered can be exploited to allow the memory content of a computer to be leaked. Such a leak could potentially expose stored passwords and other sensitive data, including personal photos, emails and instant messages.

Researchers at Google's Project Zero and academic institutions including the Graz University of Technology in Austria discovered the problem last year and disclosed it Wednesday.

There's no evidence that bad actors have yet exploited the bugs, but companies from Microsoft to Mozilla said this week they have worked to patch up vulnerabilities to their operating systems and browsers to protect against one of the bugs. Researchers say the other is harder to fix and "will haunt us for quite some time."

Here's a look at what's affected, what's being done about it and whether you should worry.

___

INTEL INSIDE

Intel is at the center of the problem because it supplies the processors used in many of the world's PCs. Researchers say one of the bugs, called Meltdown, affects nearly every processor it's made since the mid-1990s.

While security flaws are typically limited to a specific company or product, Intel says the problem is "not a bug or a flaw in Intel products" but rather a broader problem affecting processing techniques common to modern computing platforms.

Both the chipmaker and Google, which informed Intel about the vulnerability in June, said they were planning to disclose the issue next week when fixes will be available. Tech companies typically withhold details about security problems until fixes are available so that hackers wouldn't have a roadmap to exploit the flaws. But in this case, Intel was forced to disclose the problem Wednesday after British technology site The Register reported it, causing Intel's stock to fall.

Most of the immediate fixes will be limited to the Meltdown bug. The other, Spectre, is harder to fix, but also harder to exploit, making it less of an immediate threat to consumer devices.

___

OTHER CHIPMAKERS

While researchers say the Meltdown bug is limited to Intel processors, they have verified Spectre as a problem for Intel, Advanced Micro Devices and ARM processors. AMD chips are also common in PCs, while ARM chips are found in many smartphones and other internet-connected products, including cars and home appliances.

AMD said there is "near zero risk" to its own processors, either because its chips are designed differently, or security fixes for Microsoft Windows and other operating systems will take care of the problem. ARM Holdings said it's working with Intel, AMD and operating system vendors to address the problem. The ARM design is also used in Apple's mobile chips. Apple said late Thursday that all of its devices are affected, but it's already made fixes to help defend against Meltdown in laptops and phones and soon plans to release mitigations in the Safari browser to help defend against Spectre.

___

SECURING THE CLOUD

The bugs also affect cloud-computing services powering much of the internet. These services, offered by Amazon, Microsoft, Google, IBM and others, give smaller companies access to data centers, web hosting and other services they need to run their businesses. But these cloud services also use computers with the same types of problem chips.

Unauthorized access will be difficult to detect so cloud-computing providers need to act quickly to protect against these vulnerabilities, said Ryan Kalember, senior vice president of cybersecurity at Proofpoint. The good news, he said, is that major cloud providers have known about this for months and have had time to tackle the problem.

___

WHAT TO DO NEXT?

There are limits to what consumers can do now to protect their computers.

Advice from the U.S Computer Emergency Readiness Team's was grim. The federal organization says that "fully removing the vulnerability" requires replacing the hardware already embedded in millions of computing devices.

That's not to say nothing can be done.

Consumers can mitigate the underlying vulnerability by making sure they patch up their operating systems with the latest software upgrades. There are already Meltdown patches for Microsoft's Windows, Apple's macOS and Linux. Mozilla says it's also implementing a short-term mitigation that disables some capabilities of its Firefox browser. Google says

Android devices are protected if they have the latest security updates.

"If you download the latest update from Microsoft, Apple, or Linux, then the problem is fixed for you and you don't have to worry," security researcher Rob Graham said in a blog post Thursday. "If you aren't up to date, then there's a lot of other nasties out there you should probably also be worrying about."