Hardware-Level Spy Back-doors That Conspiracy Theorists Warned About Have Been Found In All Phones and Computers made by Silicon Valley

Your worst fears from 1984, The Terminator, SkyNet and all things Big Brother have been confirmed. Intel, Cisco, Google and most of Silicon Valley sold you out like a bitch. Consumers need to sue the Silicon Valley Companies into oblivion! They took billions of your consumer dollars and sold you a lie that damaged your life!

Built-in "security flaws" put virtually all phones, computers at risk - Thank You Silicon Valley

By Douglas Busvine and Stephen Nellis ,

FILE PHOTO - The Intel logo is shown at the E3 2017 Electronic Entertainment Expo in Los Angeles, California, U.S. June 13, 2017. REUTERS/ Mike Blake

More

By Douglas Busvine and Stephen Nellis

FRANKFURT/SAN FRANCISCO (Reuters) - Security researchers on Wednesday disclosed a set of security flaws that they said could let hackers steal sensitive information from nearly every modern computing device containing chips from Intel Corp <INTC.O>, Advanced Micro Devices Inc <AMD.O> and ARM Holdings.

One of the bugs is specific to Intel but another affects laptops, desktop computers, smartphones, tablets and internet servers alike. Intel and ARM insisted that the issue was not a design flaw, but it will require users to download a patch and update their operating system to fix.

Related Searches

Intel Chip Flaw

Intel Design Flaw

Intel Security Flaw

Intel Vulnerability

"Phones, PCs, everything are going to have some impact, but it'll vary from product to product," Intel CEO Brian Krzanich said in an interview with CNBC Wednesday afternoon.

Researchers with Alphabet Inc's <GOOGL.O> Google Project Zero, in conjunction with academic and industry researchers from several countries, discovered two flaws.

The first, called Meltdown, affects Intel chips and lets hackers bypass the hardware barrier between applications run by users and the computer's memory, potentially letting hackers read a computer's memory and steal passwords. The second, called Spectre, affects chips from Intel, AMD and ARM and lets hackers potentially trick otherwise error-free applications into giving up secret information.

The researchers said Apple Inc <AAPL.O> and Microsoft Corp <MSFT.O> had patches ready for users for desktop computers affected by Meltdown. Microsoft declined to comment and Apple did not immediately return requests for comment.

Daniel Gruss, one of the researchers at Graz University of Technology who discovered Meltdown, called it "probably one of the worst CPU bugs ever found" in an interview with Reuters.

Gruss said Meltdown was the more serious problem in the short term but could be decisively stopped with software patches. Spectre, the broader bug that applies to nearly all computing devices, is harder for hackers to take advantage of but less easily patched and will be a bigger problem in the long term, he said.

Speaking on CNBC, Intel's Krzanich said Google researchers told Intel of the flaws "a while ago" and that Intel had been testing fixes that device makers who use its chips will push out next week. Before the problems became public, Google on its blog said Intel and others planned to disclose the issues on Jan. 9.

The flaws were first reported by tech publication The Register. It also reported that the updates to fix the

problems could causes Intel chips to operate 5 percent to 30 percent more slowly. (http://bit.ly/2CsRxkj)

Intel denied that the patches would bog down computers based on Intel chips.

"Intel has begun providing software and firmware updates to mitigate these exploits," Intel said in a statement. "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."

ARM spokesman Phil Hughes said that patches had already been shared with the companies' partners, which include many smartphone manufacturers.

"This method only works if a certain type of malicious code is already running on a device and could at worst result in small pieces of data being accessed from privileged memory," Hughes said in an email.

AMD chips are also affected by at least one variant of a set of security flaws but that it can be patched with a software update. The company said it believes there "is near zero risk to AMD products at this time."

Google said in a blog post that Android phones running the latest security updates are protected, as are its own Nexus and Pixel phones with the latest security updates. Gmail users do not need to take any additional action to protect themselves, but users of its Chromebooks, Chrome web browser and many of its Google Cloud services will need to install updates.

The defect affects the so-called kernel memory on Intel x86 processor chips manufactured over the past decade, The Register reported citing unnamed programmers, allowing users of normal applications to discern the layout or content of protected areas on the chips.

That could make it possible for hackers to exploit other security bugs or, worse, expose secure information such as passwords, thus compromising individual computers or even entire server networks.

Dan Guido, chief executive of cyber security consulting firm Trail of Bits, said that businesses should quickly move to update vulnerable systems, saying he expects hackers to quickly develop code they can use to launch attacks that exploit the vulnerabilities. "Exploits for these bugs will be added to hacker's standard toolkits," said Guido.

Shares in Intel were down by 3.4 percent following the report but nudged back up 1.2 percent to $44.70 in after-hours trading while shares in AMD were up 1 percent to $11.77, shedding many of the gains they had made earlier in the day when reports suggested its chips were not affected.

It was not immediately clear whether Intel would face any significant financial liability arising from the reported flaw.

"The current Intel problem, if true, would likely not require CPU replacement in our opinion. However the situation is fluid," Hans Mosesmann of Rosenblatt Securities in New York said in a note, adding it could hurt the company's reputation.

(Reporting by Douglas Busvine in Frankfurt and Stephen Nellis and Salvador Rodriguez in San Francisco; Additional reporting by Jim Finkle in Toronto and Laharee Chatterjee in Bengaluru; Editing by Susan Fenton and Lisa Shumaker)

Of course they did.
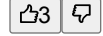
↰Reply   Replies (1)

👍4 👎

···

Nour in SD
ur20 hours ago
SDGood reporting, but leaving this part in the article "AMD NO AFFECTED" is not 100% accurate, but what is these days, right? I'm semi disappointed, but good reporting non-the-less

↰Reply   Replies (3)

👍3 👎

···

Kimona
m5hours ago
First off it's not a flaw. It was designed into the chips for the NSA. Just like Microsoft has been working with the NSA for decades to put back doors in Windows. That leaked out when Vista was been developed.

↰Reply   Replies (2)

👍10 👎2