

Intel Chose Greed Over Customer Security!

Intel warned select customers of processor vulnerabilities before the U.S. Government

By Abhay Venkatesh

@abhay_venkat4.

18



Less than a month after Intel's [massive processor vulnerabilities](#), namely Spectre and Meltdown, were revealed ahead of the planned disclosure timeline, [The Wall Street Journal reports](#) that Intel warned select customers of the flaws, but left out the U.S. Government. The flaws, [identified by the Google Project Zero team in June](#), were to be disclosed on the 9th of January, but [were revealed early](#) due to commits that were actively being made to the Linux kernel.

As per the report, initial disclosures about the vulnerabilities were made to select large customers that included U.S. companies such as Microsoft and Amazon, but also foreign companies such as ARM Holdings in the U.K., along with Lenovo and Alibaba in China.

Due to the severity of the flaws, Intel's decision to warn select customers in advance, and leaving out the U.S. Government, has

been met with concerns of the information being misused. The report states that, while there is no certain proof, sources believe it is possible that the Chinese government was aware of the communications between Intel and the Chinese tech giants, as such communications are routinely monitored by the authorities. However, an Alibaba spokesperson declined the speculation that any information was shared with the authorities. The other companies reportedly did not share information with the U.S. Government owing to a non-disclosure agreement.

An official at the Department of Homeland Security said that the staffers learned of the flaws on January 3 from news reports and not from Intel in advance, explaining [the hastily-provided mitigation](#) for the problem. The United States Computer Emergency Readiness Team (US-CERT), an organization within the Department of Homeland Security's National Protection and Programs Directorate, is often informed of such discoveries, which then handles how the information is addressed. White House cyber security coordinator Rob Joyce [tweeted earlier this month](#) revealing that the NSA wasn't privy to the information as well.

Intel's decision to warn its large customers meant that those companies had more time to plan mitigation and patching strategies. However, Intel's [patches and fixes themselves have had problems](#), forcing the [company to halt their rollout](#). [Microsoft pushed out emergency updates to disable patches](#) that were negatively impacting stability as well. Smaller partners have been impacted adversely, as they are still working to get fixes out for their customers.

According to the report, an Intel spokesperson declined to list the companies that were informed before the scheduled announcement, however, noted that the company couldn't inform all the intended parties - including the U.S. Government - as the news was revealed earlier than planned. Intel's [disclosure policy has already been questioned](#) by the U.S. Congress and the [company is being sued](#) for the processor vulnerabilities.

INTEL

SPECTRE

MELTDOWN

VULNERABILITIES

US-CERT

US GOVERNMENT