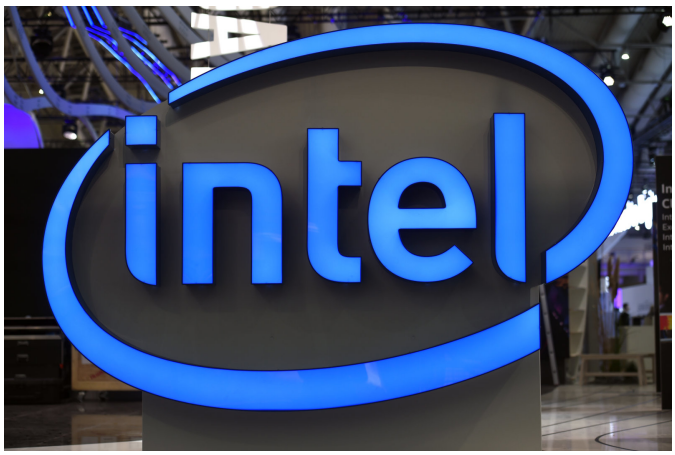
Intel eats back the words it said earlier this month as it admits newer Skylake and Kaby Lake CPUs are also affected by the patch released to fix the issues brought about Spectre and Meltdown.



According to a company blog post, while the firmware updates are "effective at mitigating exposure to the security issues," they also lead to more frequent reboots. Previously Intel insisted the issue was only noticeable on systems running on older Broadwell and Haswell CPUs, but tests have confirmed similar behaviours happen on Ivy Bridge-, Sandy Bridge-, Skywell- and Kaby Lake-based platforms.

That said, Intel insists it is close to identifying the root cause of the issue. In parallel, it is providing vendors with "beta microcode" for validation in the near future.

Furthermore, Chipzilla has an update on how the Spectre and Meltdown fixes affect datacentres-- according to initial benchmarks the two-socket Xeon Scalable systems are not affected, at least in terms of energy efficiency or performance when running Java business applications. However some operations show an impact of around 2-4%, while performance during some I/O loads is hit by a decrease of up to 25%.

Intel concludes it is working with partners and customers to address the situation, with one solution being "Retpoline," a technique developed by a Google engineer to protect the search giant's systems from a second Spectre variant without hitting performance.

Go Firmware updates and Initial Performance Data for Datacentre Systems