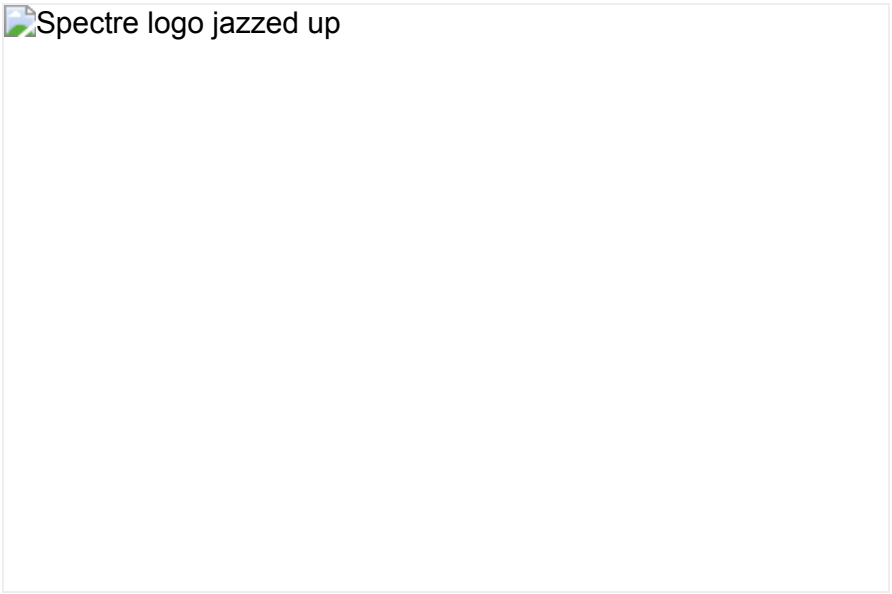
Intel admits that it soldered spy back-doors into it's hardware that were built so they could never be closed or fixed

And won’t fix Meltdown *nor* Spectre for 10 product families covering 230-plus CPUs

By Simon Sharwood, APAC Editor67 Reg comments SHARE ▼



Intel has issued fresh "microcode revision guidance" that reveals it won’t address the Meltdown and Spectre design flaws in all of its vulnerable processors – in some cases because it's too tricky to remove the Spectre v2 class of vulnerabilities.

The new guidance, issued April 2, adds a “stopped” status to Intel’s “production status” category in its array of available Meltdown and Spectre security updates. "Stopped" indicates there will be no microcode patch to kill off Meltdown and Spectre.

The guidance explains that a chipset earns “stopped” status because, “after a comprehensive investigation of the microarchitectures and microcode capabilities for these products, Intel has determined to not release microcode updates for these products for one or more reasons.”

Those reasons are given as:

> - **Micro-architectural characteristics that preclude a practical implementation of features mitigating [Spectre] Variant 2 (CVE-2017-5715)**
> - **Limited Commercially Available System Software support**
> - **Based on customer inputs, most of these products are implemented as “closed systems” and therefore are expected to have a lower likelihood of exposure to these vulnerabilities.**

Thus, if a chip family falls under one of those categories – such as Intel can't easily fix Spectre v2 in the design, or customers don't think the hardware will be exploited – it gets a "stopped" sticker. To leverage the vulnerabilities, malware needs to be running on a system, so if the computer is totally closed off from the outside world, administrators may feel it's not worth the hassle applying messy microcode, operating system, or application updates.

"Stopped" CPUs that won’t therefore get a fix are in the Bloomfield, Bloomfield Xeon, Clarksfield, Gulftown, Harpertown Xeon C0 and E0, Jasper Forest, Penryn/QC, SoFIA 3GR, Wolfdale, Wolfdale

Xeon, Yorkfield, and Yorkfield Xeon families. The new list includes various Xeons, Core CPUs, Pentiums, Celerons, and Atoms – just about everything Intel makes.

Most the CPUs listed above are oldies that went on sale between 2007 and 2011, so it is likely few remain in normal use.

Intel has not revealed which of the "stopped" CPUs listed can’t be mitigated at all, and which Chipzilla can't be bothered finishing patches for. We’ve asked Intel to provide that list, and will update this story if the biz replies.

There’s some good news in the tweaked guidance: the Arrandale, Clarkdale, Lynnfield, Nehalem, and Westmere families that were previously un-patched now have working fixes available in production, apparently.

“We’ve now completed release of microcode updates for Intel microprocessor products launched in the last 9+ years that required protection against the side-channel vulnerabilities discovered by Google Project Zero," an Intel spokesperson told *The Reg*.

"However, as indicated in our latest microcode revision guidance, we will not be providing updated microcode for a select number of older platforms for several reasons, including limited ecosystem support and customer feedback.”

ɔ-yay,
tdown CPU
s are here.
v, Spectre flaws
haunt tech
ıstry for years

READ MORE

Now all Intel has to do is sort out a bunch of lawsuits, make sure future products don't have similar problems, combat a revved-up-and-righteous AMD and Qualcomm in the data centre, find a way to get PC buyers interested in new kit again, and make sure it doesn't flub emerging markets like IoT and 5G like it flubbed the billion-a-year mobile CPU market. ®