



SIGN UP HERE

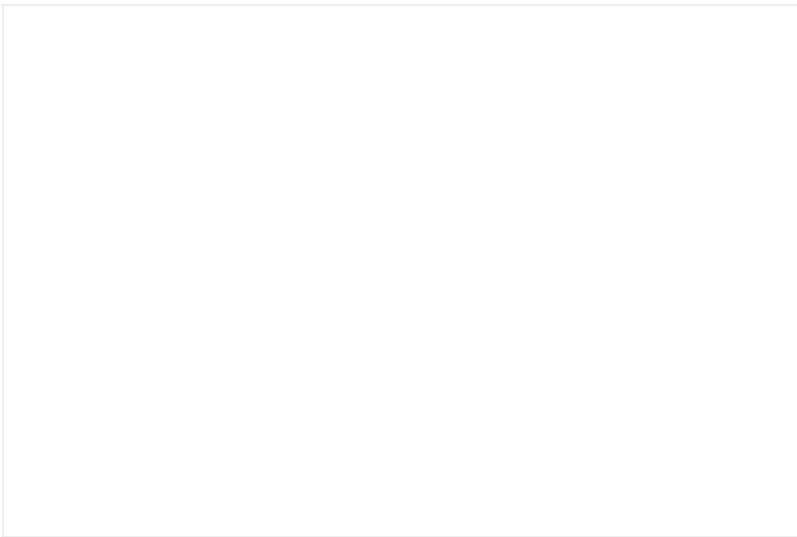
Security

# Intel admits a load of its CPUs have Spectre v2 flaw that can't be fixed

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

By [Simon Sharwood](#), APAC Editor 4 Apr 2018 at 01:15

81 [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.

Advertisement



[SIGN UP HERE](#)

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.

**Woo-yay, Meltdown CPU fixes are here. Now, Spectre flaws will haunt tech industry for years**

[READ MORE →](#)

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."

Advertisement



[SIGN UP HERE](#)


Now all Intel has to do is sort out a bunch of lawsuits, make sure future products don't have similar problems, combat a rewed-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. ®

**PS:** Chipzilla today [launched](#) some eighth-gen Core i9 parts for laptops. These are [allegedly](#) free of Spectre and Meltdown.

**Sponsored:** [Minds Mastering Machines - Call for papers now open](#)

Tips and corrections

81 Comments

 **Sign up to our Newsletter**  
Get IT in your inbox daily



## More from The Register

### Intel gives Broadwells and Haswells their Meltdown medicine

Chipzilla and Oracle are working their way back through time to deliver fixes

### Creaking Chromebooks getting Meltdown protection soon

Chrome OS 66 to protect older Intel units, still working on ARM

### Intel adopts Orwellian irony with call for fast Meltdown-Spectre action after slow patch delivery

For now, have some code that won't crash Skylakes and stay close to your Telescreens

### Azure VMs borked following Meltdown patch, er, meltdown

No ETA yet for West Europe machines

### Hands up who HASN'T sued Intel over Spectre, Meltdown chip flaws

Chipzilla says class-action lawsuit tally stands at 32

### Intel didn't tell CERTS, govts, about Meltdown and Spectre because they couldn't help fix it

Letters to Congress detail the plan to keep CPU flaws secret

## Whitepapers



#### Governance and compliance in 2017

The emphasis on data security, and the risk of data loss have all become sharpened focal points for businesses.



#### Planning for Office 365 Gaps

Plan your risk management strategy - don't just hope your email and data is protected in the cloud.



#### Continuous Improvement: The Data Management Playbook

You need more insight from more data to understand and serve increasingly powerful customers.



#### Climbing mount automation

Automation is not an impossible goal. With the right expertise, any business can plan a safe route and reach the summit.

## Sponsored links

[Get The Register's Headlines in your inbox daily - quick signup!](#)

## About us>

- [Who we are](#)
- [Under the hood](#)
- [Contact us](#)
- [Advertise with us](#)

## More content>

- [Week's headlines](#)
- [Top 20 stories](#)
- [Alerts](#)
- [Whitepapers](#)

## Situation Publishing>

- [The Next Platform](#)
- [Continuous Lifecycle London](#)
- [M-cubed](#)
- [Webinars](#)



**The Register** - Independent news and views for the tech community. Part of Situation Publishing

## Sign up to our Newsletters

Join our daily or weekly newsletters, subscribe to a specific section or set [News alerts](#)

[Subscribe](#)



Biting the hand that feeds IT © 1998–2018

[Cookies](#) [Privacy](#) [Ts&Cs](#)