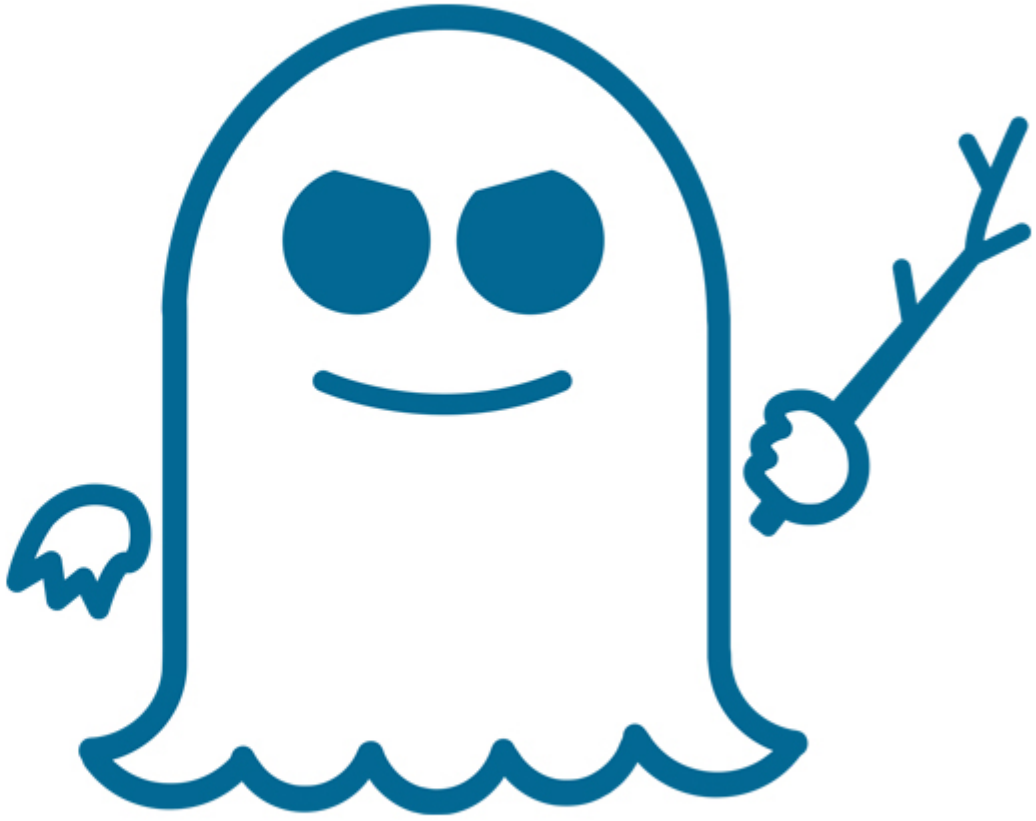


Meltdown and Spectre

SNAFU or FUBAR

Agenda

Meltdown

Spectre

What can we do about it?

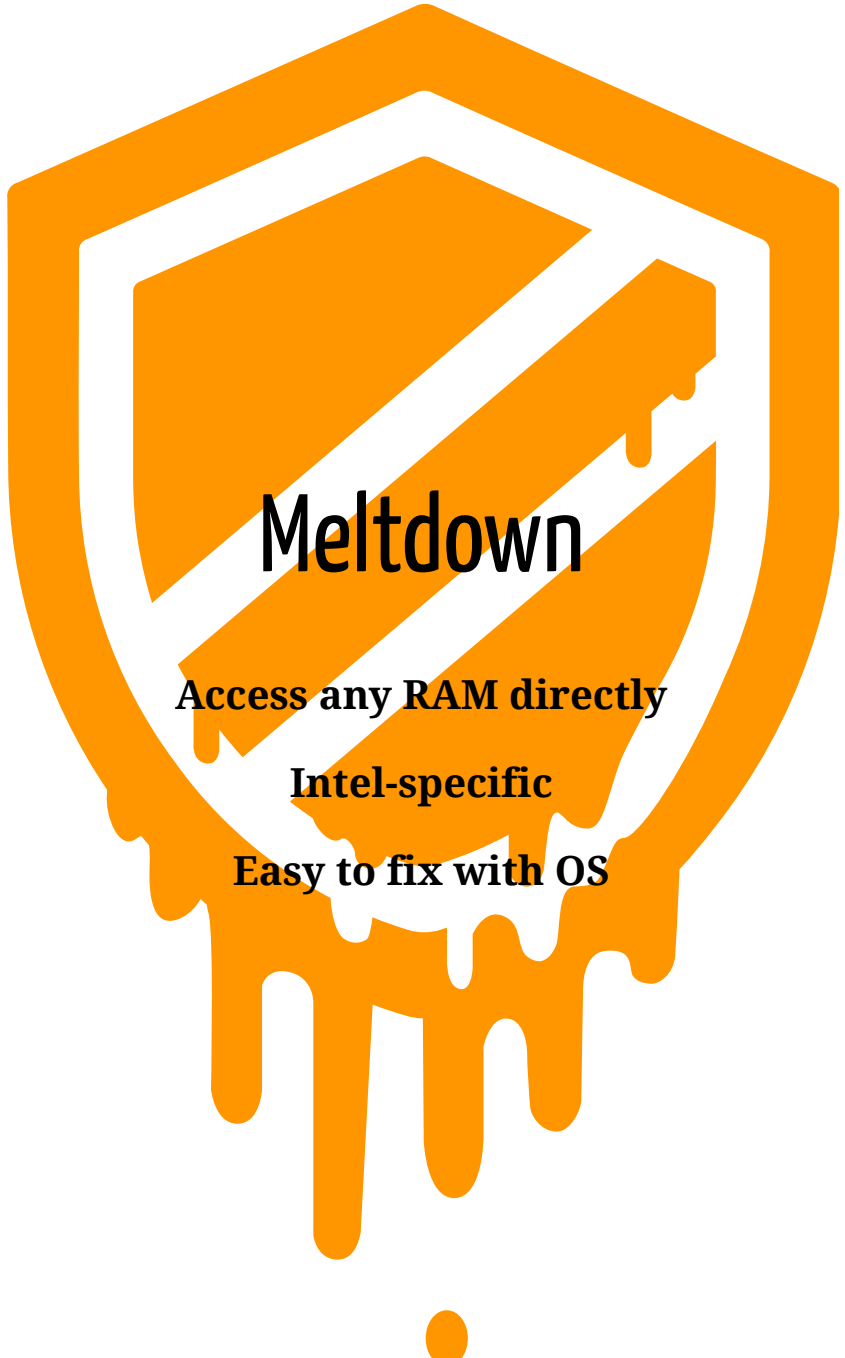
Under the hood

Processor caches

Out-of-order execution

Branch prediction

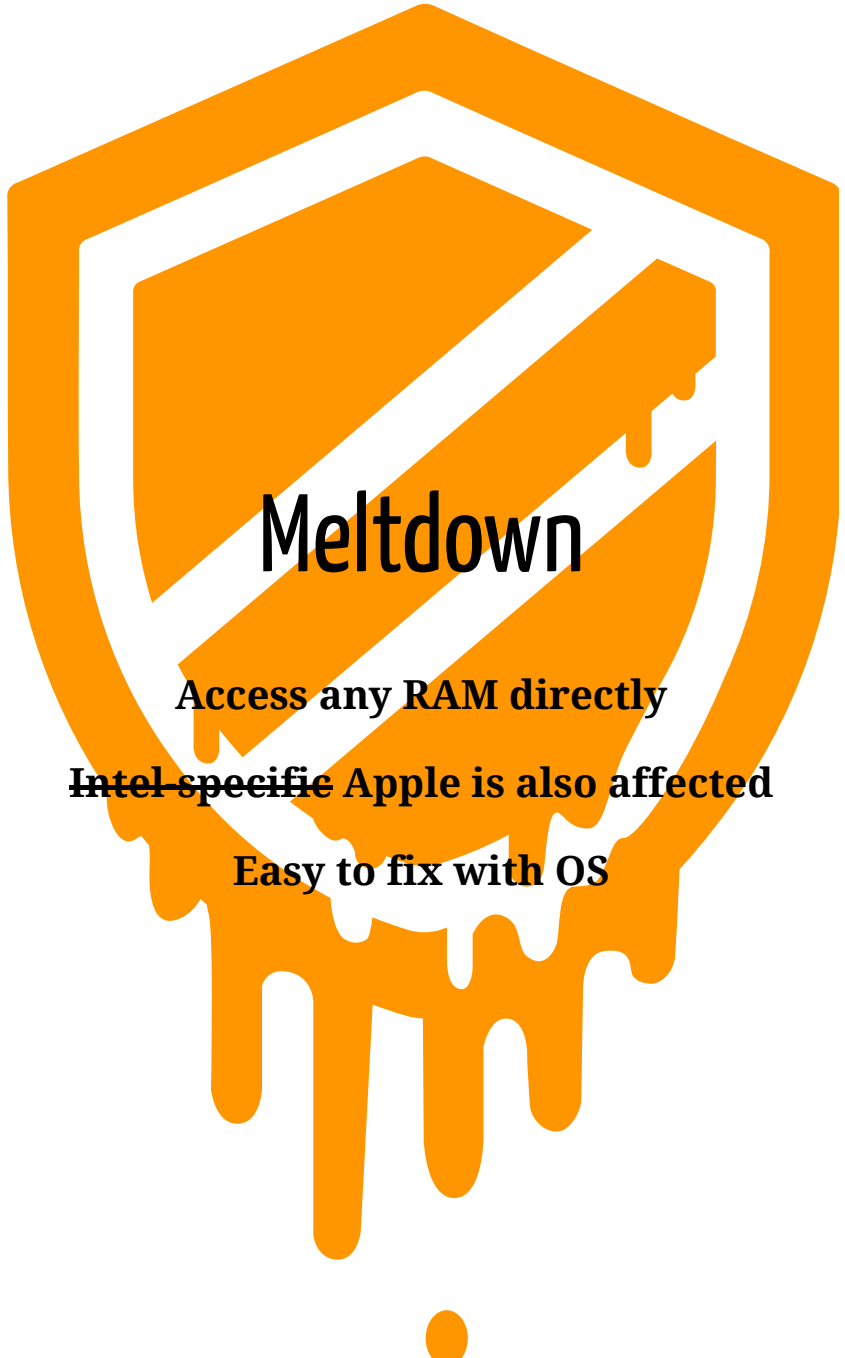
Speculative execution



Access any RAM directly

Intel-specific

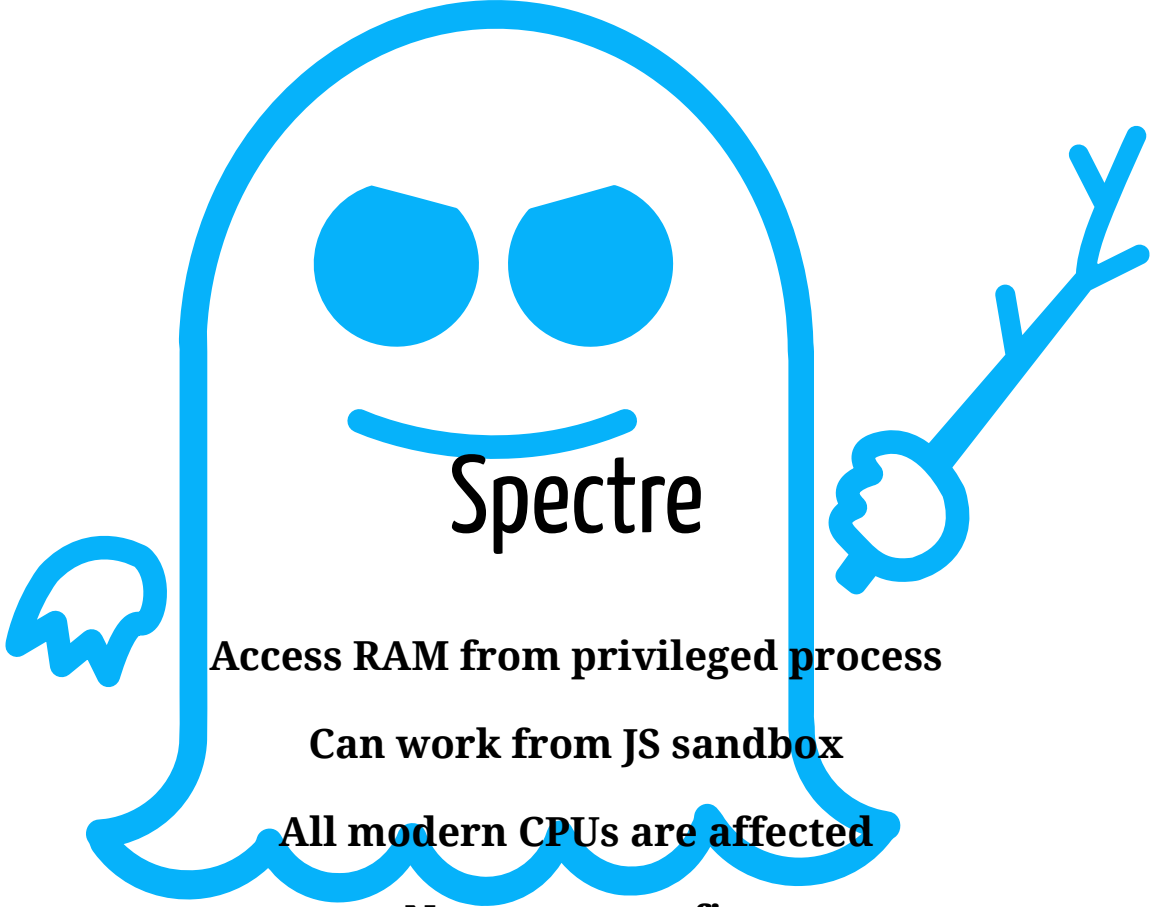
Easy to fix with OS



Access any RAM directly

~~Intel specific~~ Apple is also affected

Easy to fix with OS



Access RAM from privileged process

Can work from JS sandbox

All modern CPUs are affected

Not so easy to fix

SPECTRE

What can we do about it?

What can we do about it?

Good news

OS patches (KAISER)

Update browsers (Firefox and Chrome have been fixed)

What can we do about it?

Bad news

Accept performance loss

Check your antivirus support of the patches (yep)

Spectre will haunt us for long

So what now?

Military situational indicators progression

SNAFU

Situation Normal, All Fucked Up

Thing are running normally.

TARFUN

Things Are Really Fucked Up Now

Houston, we have a problem.

FUBAR

Fucked Up Beyond All Recognition

Burn it to the ground and start over from scratch; it's totally destroyed.

Useful links

- https://www.youtube.com/watch?v=IPhvL3A-e6E

Most complete and user-friendly explanation in 48 mins

- https://www.youtube.com/watch?v=8FFSQwrLsfE

Most complete and non user-friendly explanation in 55 mins

- https://arstechnica.com/gadgets/2018/01/meltdown-and-spectre-heres-what-intel-apple-microsoft-others-are-doing-about-it/

Meltdown and Spectre: Here's what Intel, Apple, Microsoft, others are doing about it

- https://www.ivanti.com/blog/meltdown-spectre-need-know/

The impact and potential issues with current solutions

- https://gist.github.com/a0viedo/282f9fce9cfa7fecb8edced71451a77a

A gist of useful links about Meltdown and Spectre with official reports

Questions?

And now google these

Intel Management Engine

AMD Trust Zone