If we were making cars, there would be the world's largest recall. Ever.

The newly-discovered vulnerabilities called Meltdown (basically melts security boundaries normally enforced by the hardware) and Spectre (name based on the root cause, speculative execution) affect almost every modern computer in existence, particularly those with Intel, AMD and ARM processors.

That's right, the new Fujitsu laptop I am using to write this and whatever desktop or laptop (and maybe even the smartphone or tablet) you are reading it on.

Meltdown and Spectre allow programs to steal data. While programs are typically not permitted to read data from other programs, a malicious program can exploit Meltdown and Spectre to get hold of secrets stored in the memory of other running programs. This might include your passwords stored in a password manager or browser, your personal photos, emails, instant messages and even business-critical documents.

Meltdown and Spectre work on personal computers, mobile devices, and in the cloud. Depending on the cloud provider's infrastructure, it might be possible to steal data from other customers. Yes, servers are affected.

Spectre tricks some applications into accessing arbitrary locations in their memory. Almost every system is affected by Spectre: desktops, laptops, cloud servers, as well as smartphones. More specifically, all modern processors capable of keeping many instructions in flight are potentially vulnerable. It is not easy to fix and will haunt us for a long while, until are almost all existing PCs existing today are crunched and in landfills or recycled.

Desktop, laptop, and cloud computers may be affected by Meltdown. More technically, every

Intel processor which implements out-of-order execution is potentially affected, effectively every processor since 1995 (except Intel Itanium and Intel Atom before 2013). Meltdown breaks the mechanism that keeps applications from accessing arbitrary system memory.

Both attacks use side channels to obtain information from the accessed memory location.

And all the chip companies apparently knew about this at least in June 2017 and were holding silent on it.

While chip industry giants play it down and tell us software patches are coming, the U.S.-government sponsored Computer Emergency Response Team (CERT) told us what we have to do: the only solution is to replace the vulnerable computer chips. All of them.

The argument against a recall goes like this:

1. With OS and software updates, most people will avoid attacks (most people avoid attacks anyway-- it's a lottery of the worst source)
2. No one that we know of has IRL exploited these...(yet... but announcing the vulnerabilities should encourage the bad guys to take a look)
3. Makers will now ensure future chips won't have the same problems (so the consumer is invited to buy his/her way out of this situation, caused by what any lawyer would call "professional negligence.")

We won't see any recalls which suggests Intel is more important in computing than General Motors is in automobiles. But now we know what is really INSIDE.

Go More on These Vulnerabilities

Go Forbes: The Available Fixes You Need For Those Huge Chip Hacks