Meltdown / Spectre

- 2 attacks (Meltdown/Spectre) => 3 vulnerabilities (CVE-2017-5754, CVE-2017-5753, CVE-2017-5715) affecting virtually every modern computer including smartphones, tablets, and PCs running almost any OS

- Both attacks take advantage of "speculative execution" by tricking the CPU into speculatively executing code that does read forbidden memory, so any chip that uses speculative execution is affected

- Speculative execution was designed under assumption that if it failed then it was like the attempt was never made and all effects are rolled back. This assumption turned out to be false and is the key to understanding Meltdown/Spectre

- Google reported to the affected companies about Spectre on June 1st 2017 and about Meltdown on July 28th 2017

- Meltdown: breaks/*melts* down the isolation between user applications and the operating system – allows hackers to bypass the hardware barrier between apps run by users and the computers core memory thus gaining access to secrets of other programs and the OS

- Spectre breaks the isolation between different applications, allowing attackers to trick programs into leaking their secrets by forcing them into accessing arbitrary portions of its memory – harder for hackers to take advantage of but also harder to fix

- Exploits do not leave any traces in traditional log files, hard to distinguish from regular benign applications, and starting to see malware samples taking advantage of the PoC

- Patches have been released for Meltdown and Spectre 1 but due to reboot issues, BSOD, and data loss the patches for Spectre 2 have been delayed/pulled. Spectre has also made previously patched browser vulnerabilities come back into play

- ELI5: CPU predicts you walk into a bar, you don't, and your wallet has been stolen

Preventive measures

- Someone needs physical access to your machine or trick you into installing malware via phishing or social engineering
- Chrome users can enable site isolation to ensure each website page is always put into different processes, each in a sandbox that limits what the process is allow to do
- Using NoScript or a similar program to block JavaScript by default – JavaScript PoC have been posted and starting to see malware use it in the wild
- All major browsers have decreased the resolution of "performace.now()" and disabled SharedArrayBuffer as attackers can measure how long it takes to read certain value from memory to determine if their guesses are correct
- Open external links using rel="noopener" or for FF rel="noopener norefferrer" as using target="_blank" the page lniked gains partial access to the linking page via the window.opener object and can be used for phishing

Ryan Johnson | ryanj@ucar.edu | x1724

Links / More Info

Initial public release on Meltdown and Spectre from the Project Zero team at Google
https://googleprojectzero.blogspot.nl/2018/01/reading-privileged-memory-with-side.html

Article with easy to follow explanation of Meltdown and Spectre
https://ds9a.nl/articles/posts/spectre-meltdown/

Detailed PDF about Meltdown and Spectre and mitigating the threats
https://www.renditioninfosec.com/files/Rendition_Infosec_Meltdown_and_Spectre.pdf

*Summary of patch status for Meltdown and Spectre
https://github.com/hannob/meltdownspectre-patches

Photo showing Spectre 2 fix status for AMD/Intel CPU
https://www.3dcenter.org/dateien/abbildungen/Spectre-Fix-Status-for-AMD-and-Intel.png

*Meltdown and Spectre checker for Linux
https://github.com/linuxlite/Spectre-Meltdown-Checker-Automated

*Meltdown and Spectre checker for Windows
https://www.grc.com/inspectre.htm

*PoC JavasScript code example
https://react-etc.net/page/meltdown-spectre-javascript-exploit-example

Article about the malware samples found in the wild
http://www.tomshardware.com/news/meltdown-spectre-malware-found-fortinet,36439.html

Update from Google about the progress and steps to help mitigate
https://developers.google.com/web/updates/2018/02/meltdown-spectre

Detailed page about Meltdown and Spectre with the official whitepapers
https://meltdownattack.com/
https://meltdownattack.com/meltdown.pdf
https://spectreattack.com/spectre.pdf

*Use at your own risk