Privasec RED
RED TEAMING & ADVANCED ETHICAL HACKING

Meltdown & Spectre Vulnerabilities

Fact Sheet v1.0 - 8th January 2018

Meltdown and Spectre are vulnerabilities present in most Intel, Apple, AMD, ARM chips which are used in most computers and consumer devices worldwide. Vendors are releasing patches and you should apply them as soon as you can, which might involve rebooting servers to apply them. Whilst waiting for patches, users should be careful that the sites they are visiting are legitimate/known sites.

BACKGROUND INFORMATION

Meltdown and Spectre allow attackers, where they can execute code on a system, to read sensitive information from memory by exploiting 'Speculative Execution'. This information could include passwords, login data, and cached files – usually information so sensitive it is usually hidden from user processes and programs.

Meltdown exploits an Intel-based privilege escalation flaw, and affects Intel processors, which are used in most Apple products. Spectre exploits two processor performance optimisation features (Speculative Execution and Branch Prediction), and affects Intel, Apple, AMD and ARM products.

Patches are becoming available for affected devices, and are crucial to minimising the risk of having information compromised via these vulnerabilities. Where possible, patches should be installed and applied in the following order: Anti-Virus, Operating System, System Firmware.

HOW IT WORKS

Companies have always attempted to engineer their processors be quicker at running software. To do this, they get told instructions by the operating system, and execute that code. In order to speed up the pipeline of instructions to execute, the processors attempt to 'guess' which instruction will come next (this is similar to your details being pre-filled with previously-entered information on a web form in your browser). To guess, they use something called 'Speculative Execution' which places the guessed instructions in memory, ready to be executed. If correct, they fetch the prepared code from memory and execute it. If wrong, and the instead system receives a different instruction, the CPU's have to undo the speculatively executed code, and run the intended instructions.

The issue arises when the speculative instructions are not completely 'undone' when guessed wrong, and continue to exist in little footholds of memory, for example temporary caches, to be accessed later. When an attacker attempts to read those temporary caches, an exception or error is raised, and because the instruction was acted on previously, the content of the kernel memory is shown in the exception. When this is run repeatedly, the contents of the kernel memory are dumped, allowing the attacker to read the entire memory information in plain view.

- Meltdown Example: A cloud-based system could be compromised by a remote attacker abusing a flaw in a client's website. Utilising the code-execution abilities of the running user, the attacker could then exploit the system using Meltdown, resulting in every user sharing the hardware having their information revealed.

- Spectre Example: A user on a system in an organisation has privileges that allow the execution of code on their profile. The user browses to a website that runs an ad or malicious piece of JavaScript. The JavaScript executes in the browser, and triggers the malicious code, disclosing cookies to other websites the user has visited, as they were stored in the memory compartment of the user's browser process.

WHICH TECHNOLOGY IS AFFECTED?

Meltdown affects all Intel processors since 1995 that support 'out-of-order execution', except Itanium and pre-2013 Atoms. It also affects all x86-64 'out-of-order' Intel CPUs since 2011. Spectre affects almost all devices that are running Intel, AMD and ARM processors.

Workaround patches are available now for Windows, Apple and Linux operating systems. Installing and enabling the latest updates for your local Operating System should suffice.

Infrastructure	Status
Windows Servers	Server admins should enable the kernel-user space splitting feature once patched - by default it is turned **off.**
Amazon and Google Cloud	Patches have been applied, re-boot virtual machines.
Microsoft Cloud	Patches are being applied, re-boot virtual machines after confirmation of patch.

BE AWARE OF THE PATCH SIDE EFFECTS

Depending on the processor model, software programs running and usage type of your system, users will likely experience a performance hit - especially if the system is oriented towards storage operations, high network bandwidth usage, or high system calls.

WHAT ELSE CAN BE DONE?

For users using Google Chrome browser, opt for the site isolation feature (may increase Chrome memory use). https://support.google.com/chrome/answer/7623121?hl=en-GB Firefox browser users will have a patch available shortly. Watch for any new Anti-Virus, Operating System and Firmware patches that emerge over the next few days, install and apply.

DO YOU REQUIRE ADDITIONAL ASSURANCE?

Privasec can provide you with additional assurance and peace of mind.

If you would like us to review your patching practices, perform a Penetration Test to assess potential vectors of attack or review your current network architecture, please contact us for a personalised quote.