CERT-MU

MELTDOWN & SPECTRE VULNERABILITIES

Whitepaper

Prepared By CERT-MU
January 2018

CONTENTS

1.0 INTRODUCTION

On 3rd January 2018, two security flaws dubbed as Meltdown and Spectre were unveiled by security researchers at Google's Project Zero in conjunction with academic and industry researchers from several countries. Basically, they are known as side-channel attacks and they take advantage of the ability to extract information from instructions that have executed on a CPU using the CPU cache as a side-channel.

The issues are organized into 3 variants:

- Variant 1 (CVE-2017-5753, Spectre): Bounds check bypass
- Variant 2 (CVE-2017-5715, also Spectre): Branch target injection
- Variant 3 (CVE-2017-5754, Meltdown): Rogue data cache load, memory access permission check performed after kernel memory read

Combined together, these security flaws affect virtually every modern computer, including smartphones, tablets and PCs from all vendors and running almost any operating system. The Meltdown and Spectre vulnerabilities also work in the cloud. Depending on the cloud provider's infrastructure, it might be possible to steal data from other customers

They allow programs to steal data which is currently processed on the computer. While programs are typically not allowed to read data from other programs, a malicious program can exploit Meltdown and Spectre to gain knowledge of sensitive and confidential information such a passwords, emails, pictures, instant messages and business documents stored in the memory of other running programs.

As per Daniel Gruss, one of the researchers who discovered the flaw, Meltdown is probably one of the worst CPU bugs ever found.

Security firms and vendors are releasing patches and fixes to mitigate these exploits and prevent any damage. CERT-MU will continue to actively monitor and analyze this situation for new developments and advise users accordingly.

2.0 WHAT IS THE SPECTRE ATTACK

Spectre attacks take advantage of a CPU's branch prediction capabilities. Modern CPUs include a feature called branch prediction, which speculatively executes instructions at a location that the CPU believes it will branch to. Such speculative execution helps to more fully utilise the parts of the CPU, minimising the time waiting, and therefore improving performance.

When a branch is successfully predicted, instructions will retire, which means the outcomes of the instructions such as register and memory writes will be committed. If a branch is mispredicted, the speculatively-executed instructions will be discarded, and the direct side-effects of the instructions are undone. What is not undone are the indirect side-effects, such as CPU cache changes. By measuring latency of memory access operations, the cache can be used to extract values from speculatively-executed instructions.

With Spectre variant 1 (CVE-2017-5753), the instructions after a conditional branch are speculatively executed as the result of a misprediction. With Spectre variant 2 (CVE-2017-5715), the CPU executes instructions at a location determined by a mispredicted branch target.

With both variants of the Spectre attack, the impact is that a process may leak sensitive data to other processes on a system. Spectre may also allow one part of an application to access other parts of the same process memory space that would otherwise not be permitted.

While the Spectre attack itself does not cross a user/kernel memory privilege boundary, depending on the configuration of the target platform, the Spectre attack may indirectly allow a user-space application to access and leak kernel memory.

3.0 WHAT IS THE MELTDOWN ATTACK

Meltdown is related to the Spectre attack since it also uses a cache side channel to access data that otherwise would not be available. The main difference is that it leverages out-of-order execution capabilities in modern CPUs. Like speculative execution due to branch prediction, as used by Spectre, out-of-order execution on a CPU is a technique for ensuring fullest utilisation of the CPU's parts. Although instructions may appear sequentially in the machine language, a CPU that supports out-of-order execution may execute instructions in a non-sequential manner, which can minimize the time that a CPU spends idle.

Meltdown leverages insecure behaviour that has been demonstrated in Intel CPUs and may affect CPUs from other vendors. Vulnerable CPUs allow memory reads in out-of-order instruction execution, and also contain a race condition between the raising of exceptions and the out-of-order instruction execution. The Meltdown attack reads a kernel memory value, which raises an exception because code running with user-space privileges are not permitted to directly read kernel memory. However, due to the race condition, out-of-order instructions following the faulting instruction may also execute. Even though instructions appear after the faulting instruction, out-of-order execution allows them to execute, using data retrieved from the instruction that raises the exception. By the time the exception is raised, some number of out-of-order instructions have executed. Although the raised exception causes the CPU to roll back the out-of-order instructions, the cache state is not reverted. This allows data from out-of-order instructions to persist beyond the point when the exception has been raised.

The impact of Meltdown is that a process running in user space is able to view the contents of kernel memory. Meltdown may also allow Spectre-like memory content leaking that does not cross the user/kernel privilege boundary.

The Linux kernel mitigations for Meltdown are referred to as KAISER, and subsequently KPTI, which aim to improve separation of kernel and user memory pages. Because the Spectre attacks do not cross user/kernel boundaries, the protections introduced with KAISER/KPTI do not add any protection against them.

4.0 DIFFERENCE BETWEEN MELTDOWN AND SPECTRE

Meltdown breaks the mechanism that keeps applications from accessing arbitrary system memory. Consequently, applications can access system memory. Spectre tricks other applications into accessing arbitrary locations in their memory. Both attacks use side channels to obtain the information from the accessed memory location.

The table below compares the 2 security flaws:

Features	Spectre	Meltdown
CPU mechanism for triggering	Speculative execution from branch prediction	Out-of-order execution
Affected platforms	CPUs that perform speculative execution from branch prediction	CPUs that allow memory reads in out-of-order instructions
Difficulty of successful attack	High - Requires tailoring to the software environment of the victim process	Low - Kernel memory access exploit code is mostly universal
Impact	Cross- and intra-process (including kernel) memory disclosure	Kernel memory disclosure to userspace
Software mitigations	Indirect Branch Restricted Speculation (IBRS) **Note:** This software mitigation also requires CPU microcode updates and it only mitigates Spectre variant 2	Kernel page-table isolation (KPTI)

5.0 AFFECTED SYSTEMS

5.1 Operating Systems

- Windows
- MacOS
- Linux (Fedora, Debian Linux)
- Android
- iOS
- Google Chrome OS (Chromebooks)
- CentOS

5.2 Processors

- Intel CPU’s (released since 1995)
- AMD

- ARM
- Mobile ARM

5.3 Browsers

- Google Chrome
- Mozilla Firefox
- Apple Safari

5.4 Mobile Devices

- Mobile devices running IOS version 11.2 (iPhones, Apple TV, iPads)
- Mobile devices running on Android (Samsung Galaxy, Samsung Note)
- Google supported Android devices (Nexus 5X, Nexus 6P, Pixel C, Pixel/XL, and Pixel 2/XL)
- Google Apps/ G Suite

5.5 Other Affected Systems

- Cisco
- Dell
- Fortinet
- Citrix
- Amazon
- Citrix
- Fortinet

6.0 AFFECTED CLOUD PROVIDERS

- Cloud providers which use Intel CPUs and Xen PV as virtualization without having patches applied.

- Cloud providers without real hardware virtualization, relying on containers that share one kernel, such as Docker, LXC, or OpenVZ are affected.

- Google Cloud Services including:
    - Google Cloud Dataflow
    - Google Cloud Datalab
    - Google Cloud Dataproc
    - Google Cloud Launcher
    - Google Compute Engine

7.0 MELTDOWN: TECHNICAL ATTACK DESCRIPTION

The Meltdown attack allows to read arbitrary physical memory from an unprivileged user program, comprised of building blocks. Basically, Meltdown combines the following two building blocks:

- Execution of Transient Instructions
- Transfer of the Microarchitectural State

First, an attacker makes the CPU execute a transient instruction sequence which uses an inaccessible secret value stored somewhere in physical. The transient instruction sequence acts as the transmitter of a covert channel, ultimately leaking the secret value to the attacker.

Meltdown consists of 3 steps: Step1 - The content of an attacker-chosen memory location, which is inaccessible to the attacker, is loaded into a register

Step 2 - A transient instruction accesses a cache line based on the secret content of the register.

Step 3 - The attacker uses Flush+Reload (microarchitectural side cache channel attack which detects whether a specific memory location is cached to make this microarchitectural state visible) to determine the accessed cache line and hence the secret stored at the chosen memory location.

By repeating these steps for different memory locations, the attacker can dump the kernel memory, including the entire physical memory.

8.0 SPECTRE: TECHNICAL ATTACK DESCRIPTION

Spectre attacks induce a victim to speculatively perform operations that would not occur during correct program execution and which leak the victim’s confidential information via a side channel to the adversary.

Step 1 - The attack begins with a setup phase, where the adversary performs operations that mistrain the processor to make an erroneous speculative prediction.

This phase also includes steps that help to induce speculative execution, such as performing targeted memory reads that cause the processor to evict from its cache a value that is required to determine the destination of a branching instruction.

During this phase, the adversary can also prepare a side channel that will be used for extracting the victim’s information

Step 2 - During the second phase, the processor speculatively executes instruction(s) that transfer confidential information from the victim’s context into a microarchitectural side channel.

While speculative execution can potentially expose sensitive data via a broad range of side channels, it can also read memory value at an attacker-chosen address and then perform a memory operation that modifies the cache state in a way that exposes the value.

Step 3 – The sensitive data is recovered.

9.0 IMPACT(S) OF THE ATTACKS

The attacks can allow attackers to cause execution of code with user privileges, thus leading to various impacts. The Meltdown attack allows reading of kernel memory from userspace. This can result in privilege escalation, disclosure of sensitive information, or it can weaken kernel-level protections, such as KASLR.

On the other side, the Spectre attack can allow inter-process or intra-process data leaks.

10.0 WORKAROUNDS

Patches and fixes have been released to mitigate the Meltdown and Spectre attacks. Users are advised to apply the following patches:

Intel Security Updates for Processors

Intel has already issued updates for the majority of processor products introduced within the past five years. By the end of next week, Intel expects to have issued updates for more than 90 percent of processor products introduced within the past five years. In addition, many operating system vendors, public cloud service providers, device manufacturers and others have indicated that they have already updated their products and services.

More information about the updates is available on:
https://security-center.intel.com

Microsoft Security Updates

- Microsoft has released January 2018 updates to fix the products below:
    - Internet Explorer
    - Microsoft Edge
    - Microsoft Windows
    - Microsoft Office and Microsoft Office Services and Web Apps
    - SQL Server
    - ChakraCore
    - .NET Framework
    - .NET Core
    - ASP.NET Core
    - Adobe Flash

- Latest patch released: 09th January 2018

More information about the updates is available on:
https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/858123b8-25ca-e711-a957-000d3a33cf99
https://support.microsoft.com/en-us/help/4056892/windows-10-update-kb4056892

Apple Security Updates

- Apple pushed out updates to iOS 11 and macOS with security improvements to Safari and WebKit to mitigate the effects of Spectre.
- Apple released Meltdown-specific patches for iOS (11.2), macOS (10.13.2), and tvOS (11.2).
  More information about the updates is available on:
  https://support.apple.com/en-ca/HT208401
  https://support.apple.com/en-us/HT208403

Google Security Updates

- Google's latest Security update (December 2017) includes mitigations reducing access to high precision timers that limit attacks on all known variants on ARM processors. This also fixes all Pixel Phones (assuming automatic updates are turned on), as well as Nexus 5X and 6P, as well as the Pixel C tablet.
- Google's latest Security update (December 2017) also patches Samsung Galaxy S8 and Note 8
- Google has also released patches to fix Google Cloud Infrastructure based products
  More information about the updates is available on:
  https://www.chromium.org/Home/chromium-security/ssca
  https://cloud.google.com/compute/docs/security-bulletins

Mozilla FireFox Foundation Security Advisory

- Mozilla has released patches which to fix Mozilla Firefox.
  More information about the updates is available on:
  https://www.mozilla.org/en-US/security/advisories/mfsa2018-01/

Android Security Bulletin

- The Android 2018-01-05 Security Patch Level (SPL) includes mitigations reducing access to high precision timers that limit attacks on all known variants on ARM processors. These changes were released to Android partners in December 2017.
- Latest Update: January 05, 2018
  More information about the updates is available on:
  https://source.android.com/security/bulletin/2018-01-01

Security Updates: Other Vendors

VENDORS	LINKS
Amazon	https://aws.amazon.com/security/security-bulletins/AWS-2018-013/
AMD	https://www.amd.com/en/corporate/speculative-execution
Android Open Source Project	https://source.android.com/security/bulletin/2018-01-01
Arm	https://developer.arm.com/support/security-update https://developer.arm.com/-/media/Files/pdf/Cache_Speculation_Side-channels.pdf
CentOS	https://lists.centos.org/pipermail/centos-announce/2018-January/date.html
Cisco	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180104-cpusidechannel
Citrix	https://support.citrix.com/article/CTX231399
Debian GNU/Linux	https://security-tracker.debian.org/tracker/CVE-2017-5754
Dell	http://www.dell.com/support/contents/us/en/19/article/product-support/self-support-knowledgebase/software-and-downloads/support-for-meltdown-and-spectre
Fedora Project	https://fedoramagazine.org/protect-fedora-system-meltdown/
Fortinet, Inc.	https://fortiguard.com/psirt/FG-IR-18-002
FreeBSD Project	https://www.freebsd.org/news/newsflash.html#event20180104:01

11.0 RECOMMENDED STEPS FOR PREVENTION

The following measures should be taken by users to mitigate the attack:

Home Users

- Update your operating system
- Check for firmware updates
- Update your browser
- Keep your antivirus software active and updated

Organisations

- Update your operating system
- Check for firmware updates
- Update your browser
- Keep your antivirus software active and updated
- After patching, performance may be diminished. Administrators should ensure that performance is monitored for critical applications and services, and work with their vendors and service providers to mitigate the effect if possible.
- Users/administrators are encouraged to refer to their OS Vendors for the most recent information or updates.
- Limit exposure now by locking down user authentication and access rights and ensuring only trusted software is running on these devices.

- Pay attention to who and what is accessing your most critical data and intellectual property.
- Reduce the risk of massive data loss with a blend of policy, training, proactive monitoring and software solutions.

12.0 REFERENCES

https://meltdownattack.com/

https://meltdownattack.com/meltdown.pdf

https://spectreattack.com/

https://spectreattack.com/spectre.pdf

https://security.googleblog.com/2018/01/todays-cpu-vulnerability-what-you-need.html

https://googleprojectzero.blogspot.com/2018/01/reading-privileged-memory-with-side.html

https://www.kb.cert.org/vuls/id/584653

https://cyber.wtf/2017/07/28/negative-result-reading-kernel-memory-from-user-mode/

https://github.com/IAIK/KAISER

https://gruss.cc/files/kaiser.pdf

https://gruss.cc/files/prefetch.pdf

https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=5aa90a84589282b87666f92b6c3c917c8080a9bf

https://lkml.org/lkml/2017/12/27/2

https://lkml.org/lkml/2018/1/4/615

https://lwn.net/Articles/741878/

https://lwn.net/Articles/737940/

https://lwn.net/Articles/742702/

http://pythonsweetness.tumblr.com/post/169166980422/the-mysterious-case-of-the-linux-page-table

https://nakedsecurity.sophos.com/2018/01/03/fckwit-aka-kaiser-aka-kpti-intel-cpu-flaw-needs-low-level-os-patches/

https://en.wikipedia.org/wiki/Kernel_page-table_isolation

https://chrisam.net/2018/01/04/speculative-execution-side-channel-vulnerabilities-vendor-published-info/

https://www.raspberrypi.org/blog/why-raspberry-pi-isnt-vulnerable-to-spectre-or-meltdown/

https://doublepulsar.com/important-information-about-microsoft-meltdown-cpu-security-fixes-antivirus-vendors-and-you-a852ba0292ec

https://www.mozilla.org/en-US/security/advisories/mfsa2018-01/

https://www.pcworld.com/article/3245606/security/intel-x86-cpu-kernel-bug-faq-how-it-affects-pc-mac.html

https://www.theverge.com/2018/1/9/16867068/microsoft-meltdown-spectre-security-updates-amd-pcs-issues

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

https://support.microsoft.com/en-us/help/4056892/windows-10-update-kb4056892

The Computer Emergency Response Team of Mauritius (CERT-MU)

National Computer Board
7th Floor, Stratton Court,
La Poudriere Street, Port Louis

Tel: 210 5520
Fax: 208 0119

Website: www.cert-mu.org.mu

Incident Reporting
Hotline: 800 2378
Email: incident@cert.ncb.mu

Vulnerability Reporting
Email: vulnerability@cert.ncb.mu

For Queries
Email: contact@cert.ncb.mu

Subscription to Mailing Lists
Email: subscribe@cert.ncb.mu