Security Advisory Report - OBSO-1801-01

Intel processor flaw: Meltdown and Spectre vulnerabilities (CVE-2017-5715, CVE-2017-5753, CVE-2017-5754)

Creation Date:	2018-01-04 16:22:27
Last Update:	2018-02-06 17:09:27

Summary

Meltdown and Spectre exploit critical vulnerabilities in modern processors. These hardware bugs allow programs to steal data which is currently processed on the computer. 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.

Meltdown breaks the isolation between user applications and operating system. (CVE-2017-5754)
The Meltdown technique can enable a user process to read ‘kernel’ memory, thus to potentially access sensitive information in memory.
So far Meltdown has only been proved on Intel processors.

Spectre breaks the isolation between different applications. (CVE-2017-5715, CVE-2017-5753)
Spectre covers two different exploitation techniques known as CVE-2017-5753 or "bounds check bypass" and CVE-2017-5715 or "branch target injection."
These techniques potentially make items in ‘kernel’ memory available to users by taking advantage of a delay in the time it may take the CPU to check the validity of a memory access call and thus again potentially access sensitive information in memory.

Spectre is harder to exploit but also harder to secure against. Researchers have verified it to work cross Intel, AMD, and ARM processors.

These two vulnerabilities apply to all modern processors (Intel, AMD, ARM, etc.) and consequently are present in all computing devices and operating systems.

Because these flaws cannot be fixed with a microcode update, an OS-level fix is required for the affected operating systems. The immediate solution comes in the form of a kernel Page Table Isolation (PTI), which separates the kernel’s memory from user processes. But this solution increases the kernel’s overhead, potentially causing the system to slow down depending on the task and processor model.

Details of the KAISER defense mechanism for KASLR
https://gruss.cc/files/kaiser.pdf

Good Summary, gone?
https://www.kb.cert.org/vuls/id/584653

Very detailed paper:
https://people.redhat.com/jcm/talks/FOSDEM_2018.pdf

VMWare advisory:
https://www.vmware.com/us/security/advisories/VMSA-2018-0002.html

State of Windows patches:
The Microsoft patches had a problem with some AMD processors, PCs are no longer bootable.

https://support.microsoft.com/en-us/help/4073757/protect-your-windows-devices-against-spectre-meltdown

http://www.zdnet.com/article/windows-10-meltdown-spectre-patch-new-updates-bring-fix-for-unbootable-amd-pcs/

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

State of SUSE patches:
SUSE is rolling out Spectre V2 mitigation soon using Retpolines rather than their current microcode approach
https://people.redhat.com/jcm/talks/FOSDEM_2018.pdf

Details

Intel Processors Last-level Cache Side-channel Timing Attack Arbitrary Kernel Memory Local Disclosure (Meltdown) - (CVE-2017-5754)

Intel x86-64 processors contain a flaw in the fundamental design that may allow for privileged memory to be disclosed.

The issue is related to out-of-order process execution which is used as a performance feature to speed up operations.

Using a side-channel attack to exploit the timing differences introduced by the caches, an attacker can frequently flush a targeted memory location using the clflush instruction.

Doing this and measuring the time it takes to reload data, the attacker can determine whether data was loaded into the cache by another process between flushes.

In this case, since the attacker controls the covert channel, the method to introduces the flaw, and the ability to measure the side effect.

This may allow user programs to use crafted commands to access parts of the privileged kernel memory and disclose the contents.

The impact can range from disclosing sensitive information to disclosing the specifics required to defeat kernel address space layout randomization (KASLR), a defense mechanism designed to help prevent more serious attacks.

Currently, there are no known workarounds or vendor upgrades to correct this issue directly.
However, various vendors have created workarounds to address this vulnerability.

Google notes that the KAISER defense mechanism for KASLR has the important (but inadvertent) side effect of impeding Meltdown. Google stresses that KAISER must be deployed immediately to prevent large-scale exploitation of this severe information leakage."
Google indicates that "every Intel processor which implements out-of-order execution is potentially affected, which is effectively every processor since 1995 (except Intel Itanium and Intel Atom before 2013)." This attack is independent of the operating system, and it does not rely on any software vulnerabilities.

On a press conference phone call on 2018-01-03, Intel emphasized that this is not a "procedural flaw or bug", rather it is a side-channel attack, while some news articles describe this as a "fundamental chip/processor design". As such, it is unknown if this can be patched by Intel; thus, operating system vendors are creating patches to workaround the issue.

Based on current testing, these patches may cause a fairly significant hit on CPU performance, potentially slowing down home systems, enterprise computers, and cloud service providers that use Intel chips by as much as 30%. Intel disputes this saying that most users will not observe that performance hit.

Some benchmark tests can be found here:

https://www.techspot.com/article/1554-meltdown-flaw-cpu-performance-windows/

Multiple Vendor Processors Speculative Memory Reference Functionality Arbitrary Kernel Memory Disclosure (Spectre) - (CVE-2017-5753, CVE-2017-5715)

Intel x86-64, AMD, and ARM processors contain a flaw in the handling of implicit caching that may allow for privileged memory to be disclosed.

The issues resides in the virtual memory implementation, which requires the processor to turn control of the processor to the operating system kernel to perform jobs such as writing to a file. This process has typically required the operating system kernel to be present in all virtual memory address space. When required, a program making a system call will cause the processor to switch to kernel mode, then switch back to user mode upon completion of the privileged actions. During this process, the kernel's data is 'invisible' to the user process, but in reality can be accessed.

- **(CVE-2017-5753)** Relying on the processor's branch prediction functionality, an attacker can trick the processor into speculatively loading data invoking an out-of-bounds read flaw.

- **(CVE-2017-5715)** Based on the ability for code in separate security contexts to influence each other's branch prediction, an attacker can target victim code that contains an indirect branch whose target address is loaded from memory and flush the cache line containing the target address out to main memory. Next, when the CPU reaches the indirect branch, it won't know the true destination of the jump, and it won't be able to calculate the true destination until it has finished loading the cache line back into the CPU, which takes a few hundred cycles. Therefore, there is a time window of typically over 100 cycles in which the CPU will speculatively execute instructions based on branch prediction."

This may allow userland programs to use crafted commands to access parts of the privileged kernel memory and disclose the contents via a side-channel attack. The impact can range from disclosing sensitive information to disclosing the specifics required to defeat kernel address space layout randomization (KASLR), a defense mechanism designed to help prevent more serious attacks.

Solution

Currently, there are no known workarounds or vendor upgrades to correct this issue directly. However, various vendors have created workarounds to address this vulnerability.

Since Spectre represents a whole class of attacks, there most likely cannot be a singular patch for it. While work is already being done to address special cases of the vulnerability, even the original website devoted to Spectre and Meltdown states: "As [Spectre] is not easy to fix, it will haunt us for a long time." (www.spectreattack.com)

Technical Information

In order to exploit this issue, an attacker needs to be able to cause the execution of such a vulnerable code pattern in the targeted context with an out-of-bounds index.
For this, the vulnerable code pattern must either be present in existing code, or there must be an interpreter or JIT engine that can be used to generate the vulnerable code pattern.
At the time of disclosure, Google has not identified any existing, exploitable instances of the vulnerable code pattern. Rather, their exploitation uses the eBPF interpreter or the eBPF JIT engine, which are built into the Linux kernel and accessible to normal users.

On 2017-12-26, Tom Lendacky from AMD said that AMD processors are not affected, stating that their microarchitecture "does not allow memory references, including speculative references, that access higher privileged data when running in a lesser privileged mode when that access would result in a page fault." Subsequent news articles on 2018-01-03 have suggested AMD processors may be impacted, but not as severely. Google's publication indicates that this issue impacts AMD while the second vulnerability dubbed Meltdown does not impact AMD.

Arm Processor Security Update:
https://developer.arm.com/support/security-update

This issue will impact many large cloud computing environments including Amazon EC2, Microsoft Azure, and Google Compute Engine. Amazon will patch the issue on their cloud service infrastructure on 2018-01-04, and Microsoft will patch Azure Cloud machines on 2018-01-10.

Google notes that "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."

Affected Products

Potentially all products using an Intel, AMD or ARM processor are affected by one or both vulnerabilities.

Unify products operate as closed systems, where only approved software is active.
This dramatically reduces the risk of the Spectre & Meltdown vulnerabilities to a low level where we can recommend that proactive patching of the operating systems, to mitigate risks associated with Spectre & Meltdown, is not necessary and not recommended at this point.

When Unify products are operating in a virtual environment, installing the CPU patches for the hypervisor (e.g. ESXi) is recommended.
This will protect the Unify product from any malicious code that may be active on a separate virtual machine on the same host.

Desktops and workstations that run Unify clients should be patched against these vulnerabilities to ensure that no other applications running on the same machine have access to sensitive information used by our clients.
This is particularly important for systems used to administer our products as high privileged credentials might be in use.
No noticeable performance issues are expected for Unify clients.

We are actively testing the available operating system patches and will include them in future releases of our products, along with details of any performance impact caused by these patches. This will ensure compatibility with future operating systems patches while providing for ongoing performance and stability. We will update our vulnerability advisory with additional details as new information becomes available.

Appliances:

Unify products not affected because of the processor used.

OpenScape 4000 IP Gateways and Line Cards

OpenScape Desk Phone CP 20X

OpenStage TDM pones, Desk Phones 35G Eco SIP and HFA

OpenScape Cordless phones and basestation

WL3, WL3 Plus and WSG Server

OpenStage Xpert 6010p turret N4

Unify products using Intel processors that are affected by Meltdown and Spectre

These products operate as closed systems, where only approved software is active.
This dramatically reduces the risk of the Spectre & Meltdown vulnerabilities to a low level.
At the moment no patch is necessary.
Investigation is ongoing, if an update is required this information will be distributed.
Performance tests are conducted with the current patches.

OpenScape Voice

OpenScape Enterprise Express

OpenScape 4000 Platform

VmWare / ESXi VMSA-2018-0002 patch was tested. For OS4000 running on VmWare no functional problems and only small performance degradation found.
Customers can patch their VmWare installations hosting OS4000 central host and/or OS4000 SoftGate.

OS4000 Platform Hotfix with new SUSE SLES 11 SP4 kernel in preparation.
This platform Hotfix affects all deployments and Hardware (EcoServer, OS4000 Branch, OSA500, DSCXLv2 and VmWare).

OpenScape Business X: no applications or JavaScript files can be installed, not affected

OpenScape Branch/ SBC

OpenScape Contact Center CDSS

Circuit Meeting Room (CMR)

Unify products using non-Intel processors that are affected by Spectre only.

These products operate as closed systems, where only approved software is active.
Spectre is much more difficult to exploit than Meltdown.

At the moment no patch is necessary.
Investigation is ongoing, if an update is required this information will be distributed.

OpenScape Desk Phone CP 400/ 600 run in a protected environment and do not allow untrusted applications to be downloaded on them

OpenStage phones 15, 20, 40, 60, 36G, 35G run in a protected environment and do not allow untrusted applications to be downloaded on them

OpenStage Xpert 6010p turret N5, X9

OpenScape Alarm Response (OScAR/ DAKS)
These devices were specifically developed as embedded devices with hardened operating systems that as a rule do not foresee the execution of third party applications or programs.

Unify Applications

Investigation about performance issues is ongoing. Test are planned to be finished M February.

At the moment we recommend **not** to patch the servers on which the applications run.

If patching is necessary this information will be distributed.

OpenScape Voice Trace Manager

OpenScape Voice Survival Authority

OpenScape Business S

OpenScape Common Management Portal (CMP)

OpenScape Composer

OpenScape Deployment Service (DLS)

OpenScape Accounting

OpenScape Fault Management

OpenScape Contact Center

OpenScape Contact Center Extension Concierge

OpenScape License Manager

OpenScape Xpert SM and MLC

Applications where the patches have been tested:

OpenScape 4000 Manager: no performance issues found, Linux patches can be applied.

OpenScape UC applications

The performance run executed on UC Applications Servers hosted on VMWare (ESXi 5.5) do not show any performance degradation after applying released patches on both ESXi 5.5 and the hosted OS SLES12 SP2. Thus as a general rule and in order to minimize the potential impact of these vulnerabilities, UC Application Development recommends UC Applications customers to take the following action and install all Linux & ESXi related patches available with the latest updates from appropriate vendors.

Following patches were applied for the UC performance run

ESXi 5.5: VMware_bootbank_esx-base_5.5.0-3.103.6480267.vib

SLES12SP2:

- *kernel-default-4.4.103-92.59.1 (IBM Z Series ONLY) released Thursday, 11th of January 2018*
- *kernel-default-4.4.103-92.56.1 released Thursday, 4th of January 2018*
- *kernel-firmware-20170530-21.16.1 released Thursday, 4th of January 2018*

No performance run was executed having installed UC directly on physical Servers. Therefore it is recommended **not to** install the security patches for Spectre and Meltdown on physical servers.

OpenScape Xpressions: no performance issues found, Windows patches can be applied.

Cloud Services

Circuit Backend Service is under Unify responsibility. A patch test showed no performance issues.

OpenScape Cloud is under Unify responsibility and will be updated as needed.

Other products

OpenScape SESAP: all SESAP machines are of general use, where other software can be installed. We recommend that all systems should be patched according to Microsoft recommendations. Reported performance impact is low and can be neglected for SESAP internal applications.

Mediatrix gateways, ATAs, and Sentinel are NOT vulnerable.

https://www.media5corp.com/media5-statement-meltdown-spectre-vulnerabilities/

Clients and applications

All Desktops and workstations that run Unify clients should be patched against these vulnerabilities to ensure that no other applications running on the same machine have access to sensitive information used by our clients. This is valid for mobiles, too.
This is particularly important for systems used to administer our products as high privileged credentials might be in use.

No noticeable performance issues are expected for Unify clients.

Recommended Actions

Unify Appliances:

At the moment no patch is necessary.
Investigation is ongoing, if an update is required this information will be distributed.
Updates will be indicated under "affected products"

Unify application products:

At the moment we recommend **not** to patch the servers on which the applications run.
The situation is still unstable, Microsoft patches are withdrawn, recall of the microcode by SuSE, VMWare/ ESXi patches are withdrawn, necessity of BIOS update is unclear....
Appliances that have been tested will be indicated under "affected products"

Clients and apps

All Desktops and workstations that run Unify clients should be patched

Hypervisors like ESXi need to be patched.

State of ESXi patches:

https://www.vmware.com/us/security/advisories/VMSA-2018-0002.html

https://kb.vmware.com/s/article/52345

Unify **Security checklists** should be applied to block unauthorized users from access.

References

https://meltdownattack.com/
https://meltdownattack.com/meltdown.pdfhttps://www.kb.cert.org/vuls/id/584653
https://spectreattack.com/spectre.pdf
https://www.techspot.com/news/72550-massive-security-flaw-found-almost-all-intel-cpus.html
http://www.zdnet.com/article/security-flaws-affect-every-intel-chip-since-1995-arm-processors-vulnerable/
https://www.heise.de/security/meldung/Massive-Luecke-in-Intel-CPUs-erfordert-umfassende-Patches-3931562.html
https://newsroom.intel.com/news/intel-responds-to-security-research-findings/
https://www.suse.com/support/kb/doc/?id=7022512
https://gruss.cc/files/kaiser.pdf

https://www.vmware.com/security/advisories/VMSA-2018-0002.html
https://www.theverge.com/2018/1/9/16867068/microsoft-meltdown-spectre-security-updates-amd-pcs-issues

http://cve.mitre.org/cgi-bin/cvename.cgi?name=2017-5715
http://cve.mitre.org/cgi-bin/cvename.cgi?name=2017-5753
http://cve.mitre.org/cgi-bin/cvename.cgi?name=2017-5754

http://fortune.com/2018/01/03/intel-kernel-security-flaw-amd/
http://pythonsweetness.tumblr.com/post/169166980422/the-mysterious-case-of-the-linux-page-table
http://www.kb.cert.org/vuls/id/584653
http://www.zdnet.com/article/tech-giants-scramble-to-fix-intel-processor-security-flaw/
https://lkml.org/lkml/2017/12/27/2
https://lkml.org/lkml/2017/12/4/709
https://lwn.net/Articles/740393/
https://security.googleblog.com/2018/01/todays-cpu-vulnerability-what-you-need.html
https://support.google.com/faqs/answer/7622138
https://www.theverge.com/2018/1/3/16846784/microsoft-processor-bug-windows-10-fix
https://www.axios.com/intel-is-dealing-with-a-major-chip-bug-but-full-impact-unclear-2522162631.html

Revision History

No results found.

Security Advisories are released as part of Unify's Vulnerability Intelligence Process. For more information see https://www.unify.com/security/advisories.

Contact and Disclaimer

OpenScape Baseline Security Office
obso@unify.com

Mies-van-der-Rohe Str. 6, D-80807 München
www.unify.com

The information provided in this document contains merely general descriptions or characteristics of performance which in case of actual use do not always apply as described or which may change as a result of further development of the products. An obligation to provide the respective characteristics shall only exist if expressly agreed in the terms of contract. Availability and technical specifications are subject to change without notice.
Unify, OpenScape, OpenStage and HiPath are registered trademarks of Unify Software and Solutions GmbH & Co. KG.

All other company, brand, product and service names are trademarks or registered trademarks of their respective holders.