Meltdown and Spectre Exploits

Updated 5th January 2018

Please note this document contains fast-changing, emerging information. Foundation IT Managed Service customers will receive periodic updates directly and will be contacted regarding next steps as applicable in their environment.

Overview

On the 3rd of January 2018 information on three vulnerabilities was released. The vulnerabilities are a result of the optimisations in the design of modern processors. This has been the case for several years, going back to at least 2011 and as far back as 1995 in some cases. Processors manufacturers have been aware since at least June 2017.

Successful exploitation of the vulnerabilities would allow an attacker to read the contents of memory, which would likely contain sensitive information such as credit card numbers, passwords or encryption keys.

The vulnerabilities are most commonly being reported under the names **Meltdown** and **Spectre**, however more detailed information can be found by looking up their CVE (Common Vulnerabilities and Exposures) identifiers, as below.

Meltdown

CVE-2017-5754: Rogue data cache load

Spectre

CVE-2017-5753: Bounds check bypass

CVE-2017-5715: Branch target injection

Impact

At the time of writing, there are no known instances of malware exploiting these vulnerabilities.

However, proof-of-concept code is publicly available for both the Spectre[1] and Meltdown[2] exploits, so the development of malicious code is an inevitability.

Spectre is expected to be more difficult to exploit on the basis that the implementation of the exploit must be tailored to the specifics of the process in which it executes. A successful exploit only facilitates an attacker reading the memory space of the same process.

Conversely, the implementation of a Meltdown exploit applies broadly to the functioning of CPUs and is easily implemented regardless of operating system or software environment. A successful exploit facilitates an attacker reading the entire memory space of the system.

[1] https://www.exploit-db.com/exploits/43427/
[2] https://github.com/gkaindl/meltdown-poc/blob/master/meltdown.c

Are all CPUs from all manufacturers affected?

The short answer is 'yes'. The longer answer is available in the table below.

Vulnerability	Has one or more CPU models which are vulnerable?		
	Intel [3]	AMD [4]	ARM [5]
CVE-2017-5754: Rogue data cache load (**Meltdown**)	Yes	No	Yes – but only for a CPI that is yet to start shipping.
CVE-2017-5753: Bounds check bypass (**Spectre**)	Yes	Yes – however, this can be resolved by OS patches and no CPU microcode update is required.	Yes
CVE-2017-5715: Branch target injection (**Spectre**)	Yes	Maybe – in theory exploitation is possible, but to date it has not been demonstrated in practice.	Yes

[3] https://www.intel.com/content/www/us/en/architecture-and-technology/facts-about-side-channel-analysis-and-intel-products.html
[4] https://www.amd.com/en/corporate/speculative-execution
[5] https://developer.arm.com/support/security-update

Mitigation

Spectre

CVE-2017-5753: Bounds check bypass

Mitigation requires analysis and rework of vulnerable application code. The most pressing requirement is for this to be done in web browsers, which offer the easiest avenue for a large-scale attack.

As part of the patches mentioned below under 'Microsoft Windows', Microsoft have made changes to the Microsoft Edge and Internet Explorer 11 browsers[6] to mitigate any potential attacks.

Mozilla have released an advisory stating that versions of Firefox older than 57 (released 14th November 2017) are vulnerable to this attack.[7]

Chrome version 64, due to be released 23rd January 2018, will contain mitigations against this attack. Until then, Chrome users can enable Site Isolation to reduce the impact of any attack.[8]

CVE-2017-5715: Branch target injection

Mitigation requires use of an operating system kernel with countermeasures built in to it. If you are using an Intel Skylake or newer CPU then you must also apply the forthcoming microcode update once released by Intel. See 'Operating System and Kernel Updates' below.

Meltdown

CVE-2017-5754: Rogue data cache load

Mitigation requires use of an operating system that separates kernel and user memory spaces. See 'Operating System and Kernel Updates' below.

[6] https://blogs.windows.com/msedgedev/2018/01/03/speculative-execution-mitigations-microsoft-edge-internet-explorer/
[7] https://blog.mozilla.org/security/2018/01/03/mitigations-landing-new-class-timing-attack/
[8] https://support.google.com/faqs/answer/7622138

Operating System and Kernel Updates

Microsoft Windows

Microsoft have released an out-of-band update for: Windows 10, Windows 8.1, Windows 7 SP1, Windows Server 2016, Windows Server 2012 R2 and Windows Server 2008 R2.

The KBs are as follows:

KB4056888 – Windows 10 Build 1511

KB4056891 – Windows 10 Build 1703

KB4056890 – Windows 10 & Windows Server 2016 Build 1706

KB4056892 – Windows 10 & Windows Server 2016 Build 1709

KB4056898 – Windows 8.1 & Windows Sever 2012 R2

KB4056897 – Windows 7 SP1, Windows Server 2008 R2 SP1

Redhat Enterprise Linux

Redhat have released updates for RHEL 7, 7.3, 7.2, 6, 6.7, 6.6, 6.5, 6.4, 5, 5.9 and OpenStack v6 – v12[9]

VMware

VMware released patches in November and December 2017 to mitigate against Spectre vulnerabilities.[10]

[9] https://access.redhat.com/security/vulnerabilities/speculativeexecution?sc_cid=701f2000000tsLNAAY&
[10] https://www.vmware.com/us/security/advisories/VMSA-2018-0002.html

Impact of Applying Patches

Performance

Mitigating against Meltdown is expected to have a performance impact on patched systems. The extent will depend directly on the amount of time a given application spends in user space vs. making system calls and the presence of CPU features such as PCID.

At the time of writing, the real-world extent is unknown. Linus Torvalds, principal developer of the Linux kernel, has suggested a 5% impact[11]. Willy Tarreau, CTO of HAProxy, has suggested a 17% impact for their application based on synthetic tests[12]. Other benchmarks have suggested between 0% and 30% can be expected. End-users are expected to see the smallest impact with server workloads seeing the most.

Patches to the Linux kernel are not imposing Page Table Isolation (PTI) fixes on AMD CPUs, given AMD's position on their chips susceptibility to Meltdown[13], so Linux on AMD processors should see no performance impact.

Anti-virus Products on Windows

Given the significant change to memory management in Windows following mitigation patches being applied, some anti-virus software is liable to trigger BSODs (Blue Screen of Death) unless it has been updated to take account of the changes in Windows.

To protect against this, Windows Update will not offer the new patches where the following registry key has not been set to the value indicated:

Key: `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\QualityCompat`

Value: `cadca5fe-87d3-4b96-b7fb-a231484277cc`

Once anti-virus vendors issue compatible updates, their software should set this value to indicate it is safe to proceed with installation of the patches. At the time of writing, 20 of 27 well-known anti-virus vendors have released updates to implement the correct behaviour in their product.

[11] https://lkml.org/lkml/2018/1/2/703
[12] https://lkml.org/lkml/2018/1/3/281
[13] https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=00a5ae218d57741088068799b810416ac249a9ce&utm_source=anz