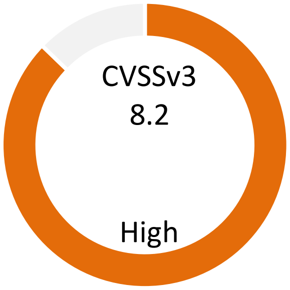
Side-Channel Speculative Execution Vulnerabilities
January 2018



Advisory ID:	nutanix-sa-007-specexvul	CVE-2017-5715 CVE-2017-5753 CVE-2017-5754
Last Updated:	4 January 2018	
Published:	4 January 2018	
Version:	1.0	

Summary

The recent media articles on CVE-2017-5715, 5753 and 5754, more recently known as Spectre and Meltdown, focus on flaws or vulnerabilities in a modern processor technique known as Speculative Execution and Branch Prediction. Vulnerability explanations and their associated technical descriptions often assume a high degree of technical expertise in the reader. However, to properly understand the ramifications and actual threat vectors of these vulnerabilities one must understand what Speculative Execution is, and what they provide in today's computing platforms.

Speculative Execution is the ability of a processor to make reasonable guesses about the future program flow. If the guess is correct then execution has been sped up for that series of instructions. If that guess is incorrect then those paths are cancelled and state changes (registers, memory, etc) are reverted. However, speculative execution also has other side effects such as cache loads, which are not reverted, which can allow for side-channel attacks to leak information. These vulnerabilities are divided into three distinct variants, listed below.

Variant 1 (Spectre) – Bounds Check Bypass (CVE-2017-5753 - CVSSv3 8.2)
Variant 2 (Spectre) – Branch Target Injection (CVE-2017-5715 - CVSSv3 8.2)
Variant 3 (Meltdown) – Rogue Data Cache Load (CVE-2017-5754 - CVSSv3 7.9)

Spectre has been used against multiple processor types to date, including Intel, AMD and ARM, while Meltdown is specifically an Intel processor vulnerability that exploits privilege escalation specific to Intel processors only. Each variant has slightly different ramifications and threat vectors associated with them.

If you would like an in-depth technical overview of the variants and methodology used to exploit them we recommend reading the Google Project Zero documentation, linked in the Sources section at the end of this document.

Actual Vectors and Their Impact

Understanding exactly how each variant can be exploited is a key to understanding the method in which you need to patch your datacenter. Each offers a slightly different vector to protect against and each have specific scenarios in which one is vulnerable.

First, one needs to divide systems into virtual vs. bare metal, which naturally divides those sets into user VMs (UVMs) vs. Hypervisors. Since mitigations to this vulnerability, specifically variant 2, rely on a new processor feature provided by microcode update, the separation of bare metal vs. virtual is necessary since in a virtual environment the hypervisor expose the new feature through to the user VM. Without this interaction (hypervisor exposing the new feature) a true fix to variant 2 is not fully possible.

Variant 1 and Variant 2

Both variant 1 and 2 rely on a malicious attacker manipulating speculative execution of known code. Collectively these two are known as Spectre and both exploit the ability to force a speculative execution in the processor out of bounds, assumingly to an attacker steered location in kernel memory. If the instructions are reordered in a way that the out-of-bounds read (branch prediction) happens prior to its determining operation the value of the out-of-bounds read is stored in cache. Then an attacker, by way of a timing attack, can determine the value resulting in kernel memory leaking.

Variant 3

This variant also uses speculative execution as a jumping off platform, however with a slightly different approach. Variant 3, also known as Meltdown, relies on lack of stringent page table permission checks in the speculative execution path. This exploit relies on the fact that during speculative execution of instruction permission faults, exceptions triggered are suppressed until completion of the whole instruction block. Any subsequent memory access may allocate into L1 cache, even if they reference inaccessible memory locations. As a result, a malicious attacker could read privileged memory by conducting targeted cache side-channel attacks.

Approach to Patching

Nutanix offers you the ability to utilize a hypervisor of your choosing, and as such one must consult with the vendor of choice. Please refer to the tables in the Affected Products section for links and information on patching either AHV, VMware ESXi, Citrix XenServer or Microsoft Hyper-V on your Nutanix cluster.

UVMs require updates available from the specific general-purpose operating system vendor in use. A list of all possible operating system vendors and their documentation on these vulnerabilities is beyond the scope of this advisory.

Virtual appliances, unlike a general-purpose system, are more purpose built virtual machines with a tighter controlled set of applications and executed code. In many cases, these types of virtual machines do not run unknown user space code. Please consult with the vendor specific to the virtual appliance in question for more information.

Affected Products

Nutanix has confirmed which software versions are affected by this vulnerability. This document will be updated with the patch release schedules. Please check the Nutanix Support Portal for the latest update.

Nutanix Products

Product	Fix Release
AHV	*Fix has been created and we will update the release timeline on Monday January 8th.*
AOS	*Evaluating if patches are needed.*
AFS	*Evaluating if patches are needed.*
Prism Central	*Evaluating if patches are needed.*
X-Ray	*Evaluating if patches are needed.*
Foundation Standalone	*Evaluating if patches are needed.*

Third-Party Products

Third Party Product	Fix Release
VMware ESXi version 5.5	See guidance available in VMware Security Advisory VMSA-2018-0002. Link in Sources section below.
VMware ESXi version 6.0	
VMware ESXi version 6.5	
Microsoft Hyper-V (All Supported Versions)	See guidance available in Microsoft Advisory ADV180002. Link in Sources section below.
Citrix XenServer (All Supported Versions)	See guidance available in Citrix Advisory CTX231390. Link in Sources section below.

Workaround

None

Timing of Advisory Release

These vulnerabilities were covered under an industry established embargo period that was scheduled to lift on January 9th 2018. However, many vendors and industry experts have decided to post information prior to the official lifting of that embargo due to media attention and some misinformation present in the mainstream.

Our policy here at Nutanix is to respect those embargos for both consumer protection, and in the interest of mutually beneficial relationships with other vendors and security researchers. After the posting of the Google Project Zero results publicly, and subsequent publishing of the spectreattack.com website it was decided to break embargo with the other entities and ensure our customers had the most up to date information.

Sources

SpectreAttack.com - Industry created website to aggregate research data.
Meltdown Academic Paper - https://meltdownattack.com/meltdown.pdf
Spectre Academic Paper - https://spectreattack.com/spectre.pdf
Intel Security Advisory (INTEL-SA-00088) - https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00088&languageid=en-fr
Microsoft Security Advisory (ADV180002) - https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV180002
Citrix Security Advisory (CTX231390) - https://support.citrix.com/article/CTX231390
Google Project Zero - https://googleprojectzero.blogspot.co.at/2018/01/reading-privileged-memory-with-side.html
Red Hat Advisory - https://access.redhat.com/security/vulnerabilities/speculativeexecution
VMware Security Advisory - https://www.vmware.com/us/security/advisories/VMSA-2018-0002.html
Cert Advisory (VU#584653) - http://www.kb.cert.org/vuls/id/584653
CVE-2017-5753 - http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2017-5753
CVE-2017-5715 - http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2017-5715
CVE-2017-5754 – http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2017-5754

If you have questions, please open a case with Nutanix Support at http://portal.nutanix.com, or by calling Support at the phone numbers on the website http://www.nutanix.com/support.

Thank you for being a Nutanix customer.

Revision History

Version	Description	Section	Date
1.0	Initial release	-	04 January 2018