VMware Response to Speculative Execution security issues, CVE-2017-5753, CVE-2017-5715, CVE-2017-5754 (aka Spectre and Meltdown) (52245)

Document Id

52245

Purpose

The purpose of this article is to describe the issues related to speculative execution in modern-day processors as they apply to VMware and then highlight VMware's response.

For VMware, the mitigations fall into 3 different categories:

- Hypervisor-Specific Mitigation
- Hypervisor-Assisted Guest Mitigation
- Operating System-Specific Mitigations

Additionally, VMware is mitigating these issues in its services.

This Knowledge Base article will be updated as new information becomes available.

Introduction

On January 3, 2018, it became public (https://meltdownattack.com/) that CPU data cache timing can be abused by software to efficiently leak information out of mis-speculated CPU execution, leading to (at worst) arbitrary virtual memory read vulnerabilities across local security boundaries in various contexts. Three variants have been recently discovered by Google Project Zero and other security researchers; these can affect many modern processors, including certain processors by Intel, AMD and ARM:

- Variant 1: bounds check bypass (CVE-2017-5753) – a.k.a. Spectre
- Variant 2: branch target injection (CVE-2017-5715) – a.k.a. Spectre
- Variant 3: rogue data cache load (CVE-2017-5754) – a.k.a. Meltdown

Operating systems (OS), virtual machines, virtual appliances, hypervisors, server firmware, and CPU microcode must all be patched or upgraded for effective mitigation of these known variants. General purpose operating systems are adding several mitigations for them. Most operating system mitigations can be applied to unpatched CPUs (and hypervisors) and will significantly reduce the attack surface. However, some operating system mitigations will be more effective when a new speculative-execution control mechanism is provided by updated CPU microcode (and virtualized to VMs by hypervisors). There can be a performance impact when an operating system applies the above mitigations; consult the specific OS vendor for more details.

Hypervisor-Specific Mitigation

Mitigates leakage from the hypervisor or guest VMs into a malicious guest VM. VMware's hypervisor products are affected by the known examples of variant 1 and variant 2 vulnerabilities and do require the associated mitigations. Known examples of variant 3 do not affect VMware hypervisor products.

VMware hypervisors do not require the new speculative-execution control mechanism to achieve this class of mitigation and therefore these types of updates can be installed on any currently supported processor. No significant performance degradation is expected for VMware's hypervisor-specific mitigations.

Hypervisor-Assisted Guest Mitigation

It virtualizes the new speculative-execution control mechanism for guest VMs so that a Guest OS can mitigate leakage between processes within the VM. This mitigation requires that specific microcode patches that provide the mechanism are already applied to a system's processor(s) either by ESXi or by a firmware/BIOS update from the system vendor. The ESXi patches for this mitigation will include all available microcode patches at the time of release and the appropriate one will be applied automatically if the system firmware has not already done so.
No significant additional overhead is expected by virtualizing the speculative-execution control mechanism in the hypervisor. There can be a performance impact when an operating system applies this mitigation; consult the specific OS vendor for more details.

Operating System-Specific Mitigations

Mitigations for Operating Systems(OSes) are provided by your OS Vendors. In the case of virtual appliances, your virtual appliance vendor will need to integrate these into their appliances and provide an updated appliance.

VMware Software-as-a-Service (SaaS) Status Updates

VMware is in the process of investigating and patching its services. The current status is found in the Resolution section.

Resolution

Hypervisor-Specific Mitigation

Specific versions of VMware vSphere ESXi (5.5, 6.0, 6.5, VMC), VMware Workstation (12.x, 14.x), and VMware Fusion (8.x, 10.x) have already been updated with hypervisor-specific mitigation as indicated in further detail by VMSA-2018-0002 (https://www.vmware.com/us/security/advisories/VMSA-2018-0002.html).

Please note that all provided VMware hypervisor-specific mitigations mentioned in this Knowledge Base article can only address known examples of the variant 1 and variant 2 vulnerabilities; known variant 3 examples do not affect VMware hypervisors. VMware will remain vigilant in updating our mitigations as new speculative-execution vulnerabilities are uncovered and as new CPU vendor microcode becomes available.

Hypervisor-Assisted Guest Mitigation

Hypervisor-Assisted Guest Mitigation patches are available. Mitigation requirements including patches have been announced in VMSA-2018-0004 (https://www.vmware.com/us/security/advisories/VMSA-2018-0004.html). Detailed instructions on enabling Hypervisor-Assisted Guest Mitigation can be found in
Hypervisor-Assisted Guest Mitigation for branch target injection (52085) (https://kb.vmware.com/s/article/52085).

Operating System-Specific Mitigations

VMware Virtual Appliances
VMware virtual appliance information can be found here: https://kb.vmware.com/s/article/52264 (https://kb.vmware.com/s/article/52264)

Photon OS
Photon OS has begun releasing fixes which are documented in
Photon OS Security Advisories (https://github.com/vmware/photon/wiki/Security-Advisories).
PHSA-2018-1.0-0097 (https://github.com/vmware/photon/wiki/Security-Updates-1.0-97)
PHSA-2018-2.0-0010 (https://github.com/vmware/photon/wiki/Security-Updates-2-10)
PHSA-2018-1.0-0098 (https://github.com/vmware/photon/wiki/Security-Updates-1.0-98)
PHSA-2018-2.0-0011 (https://github.com/vmware/photon/wiki/Security-Updates-2-11)

VMware products that are installed and run on Windows
VMware products that run on Windows might be affected if Windows has not been patched with appropriate updates. VMware recommends that customers contact Microsoft for resolution.

VMware products that are installed and run on Linux (excluding virtual appliances), Mac OS, iOS or Android
VMware products that run on Linux (excluding virtual appliances), Mac OS, iOS, or Android might be affected if the operating system has not been patched with appropriate updates. VMware recommends that customers contact their operating system vendor for resolution.

VMware Software-as-a-Service (SaaS) Status Updates

Air-Watch
https://support.air-watch.com/articles/115015960907 (https://support.air-watch.com/articles/115015960907)
https://support.air-watch.com/articles/115015960887 (https://support.air-watch.com/articles/115015960887)

VMware Horizon Cloud
http://status.horizon.vmware.com/incidents/nd1ry9frbkvq (http://status.horizon.vmware.com/incidents/nd1ry9frbkvq)

VMware Cloud on AWS
https://status.vmware-services.io (https://status.vmware-services.io/)

VMware Identity Manager SaaS
http://status.vmwareidentity.com (http://status.vmwareidentity.com/)

Request a Product Feature

To request a new product feature or to provide feedback on a VMware product, please visit the Request a Product Feature (http://www.vmware.com/contact/contactus.html?department=prod_request) page.

Feedback

Did this article help you?

- This article resolved my issue.
- This article did not resolve my issue.
- This article helped but additional information was required to resolve my issue.

* (required) What can we do to improve this information? (4000 or fewer characters)

Email Id

Submit