NATIONAL SECURITY AGENCY
CYBERSECURITY ADVISORY

VULNERABILITIES AFFECTING MODERN PROCESSORS

DISCUSSION

Three vulnerabilities affecting modern Intel®[a] [1], AMD®[b] [2], and ARM®[c] processors have been disclosed. CVE®[3]-2017-5753 (bounds check bypass) and CVE-2017-5715 (branch target injection), also known as Spectre[4], have been confirmed to affect Intel, AMD, and ARM processors. CVE-2017-5754 (rogue data cache load), also known as Meltdown[4], has been confirmed to affect Intel processors. The vulnerabilities could be leveraged to read privileged system memory from an unprivileged context. The vulnerable processors are present in systems widely used across the Department of Defense (DoD). Software patches have been released by vendors to mitigate the hardware vulnerabilities.

MITIGATION ACTIONS

There are no fundamental hardware mitigations available to fix the associated architectural vulnerabilities, so software patches must be applied. Install patches and upgrade to new software versions that mitigate the vulnerabilities as those patches and software become available. Firmware patches are pending release from Original Equipment Manufacturers (OEMs).

OPERATING SYSTEMS

Windows

Microsoft®[d] released an advisory[5] and guidance[6] for Spectre and Meltdown. Install patches for Windows 10 and Windows Server 2016 released on January 3, 2018. Install patch 4056892[7] for Windows 10 1709. Install patch 4056891[8] for Windows 10 1703. Install patch 4056890[9] for Windows 10 1607 and Windows Server 2016. Install patch 4056888[10] for Windows 10 1511. Install patch 4056893[11] for Windows 10 1507. Install all patches released during the January 2018 Patch Tuesday, when made available on or around January 9, to mitigate other Windows operating systems.

[1] Intel Responds to Security Research Findings. https://newsroom.intel.com/news/intel-responds-to-security-research-findings/
[2] An Update on AMD Processor Security. https://www.amd.com/en/corporate/speculative-execution
[3] CVE is a registered trademark of The MITRE Corporation
[4] Spectre and Meltdown Attacks. https://spectreattack.com/ and https://meltdownattack.com/
[5] ADV180002 | Guidance to mitigate speculative execution side-channel vulnerabilities. https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/ADV180002
[6] Windows Client Guidance for IT Pros to protect against speculative execution side-channel vulnerabilities. https://support.microsoft.com/en-us/help/4073119/windows-client-guidance-for-it-pros-to-protect-against-speculative-exe
[7] https://support.microsoft.com/en-us/help/4056892
[8] https://support.microsoft.com/en-us/help/4056891
[9] https://support.microsoft.com/en-us/help/4056890
[10] https://support.microsoft.com/en-us/help/4056888
[11] https://support.microsoft.com/en-us/help/4056893

Installation of the applicable patch may result in operating system stability issues due to antivirus applications that make unsupported calls into kernel memory. Due to the stability issue, the patch will not install until a specific registry value exists on a system[12]:

```
Key: HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\QualityCompat
Value Name: cadca5fe-87d3-4b96-b7fb-a231484277cc

Value Type: REG_DWORD
Value Data: 0
```

Contact antivirus vendors to confirm whether a specific antivirus product is compatible with the patch. The registry value may be created by installation of an antivirus product update. The registry value can also be deployed enterprise wide using Group Policy Registry Preferences if the antivirus product in use is known to be compatible with the patch.

See McAfee KB90167[13] for more information about McAfee product minimum version requirements affecting Host Based Security System (HBSS) deployments in DoD. See Symantec TechNote TECH248545[14] for more information about Symantec Endpoint Protection product minimum version requirements.

Linux® [e]

Upgrade to Linux kernel 4.14.11 released on January 3, 2018 which has Kernel Page-Table Isolation (KPTI), previously known as KAISER, patches incorporated. Linux kernel version 4.15 released on or around January 21, 2018 also incorporates the KPTI patches.

macOS™ [f]

Upgrade to macOS 10.13.2 High Sierra released on December 6, 2017[15]. Upgrade to 10.13.3, when made available, for a complete mitigation.

Android™ [g]

Install patch 2018-01-05 on Android-based devices[16].

Chrome OS™ [h]

Upgrade to Chrome OS 63 and above released on December 15, 2017[17].

BROWSERS

Edge™ [i] and Internet Explorer™ [j]

Install previously mentioned patches for Windows 10 and Windows Server 2016 as well as all patches released for the January 2018 Patch Tuesday[18].

[12] Important information regarding the Windows security updates released on January 3, 2018 and anti-virus software. https://support.microsoft.com/en-us/help/4072699
[13] Meltdown and Spectre – Microsoft update (January 3, 2018) compatibility issue with anti-virus products. https://kc.mcafee.com/corporate/index?page=content&id=KB90167
[14] Blue Screen of Death with Stop Code: MEMORY_MANAGEMENT (0x1a) After Applying Windows Security Updates from 01/03/2018. https://support.symantec.com/en_US/article.TECH258545.html
[15] About the security content of macOS High Sierra 10.13.2, Security Update 2017-002 Sierra, and Security Update 2017-005 El Capitan. https://support.apple.com/en-us/HT208331
[16] Android Security Bulletin - January 2018. https://source.android.com/security/bulletin/2018-01-01
[17] Google's Mitigation Against CPU Speculative Execution Attack Methods. https://support.google.com/faqs/answer/7622138
[18] Mitigating speculative execution side-channel attacks in Microsoft Edge and Internet Explorer. https://blogs.windows.com/msedgedev/2018/01/03/speculative-execution-mitigations-microsoft-edge-internet-explorer/

Chrome™ [k]

Upgrade to Chrome 64 when released on or around January 23, 2018. The Site Isolation[19] feature, introduced in Chrome 63, can also be used as a mitigation but may cause 10-20% more memory usage and some sites may not work correctly. Visit chrome://flags#enable-site-per-process in the browser, click Enable next to Strict site isolation, and restart the browser[20]. Site Isolation can also be configured via enterprise policy[21] using the latest policy templates[22].

Firefox™ [l]

Upgrade to at least Firefox 57 released on November 14, 2017[23].

VIRTUALIZATION

VMware® [m]

Upgrade ESXi 6.5 to patch ESXi650-201712101-SG, Upgrade ESXi 6.0 to patch ESXi600-201711101-SG. Upgrade ESXi 5.5 to ESXi550-201709101-SG. Note that ESXi 5.5 will remain vulnerable CVE-2017-5753. Customers running ESXi 5.5 should consider upgrade 6.0 or 6.5 with the patches applied for a complete mitigation. VMware Workstation 14 is not affected. Upgrade to VMware Workstation 12 to 12.5.8 on all operating systems. VMware Fusion 10 is not affected. Upgrade VMware Fusion 8 to 8.5.9 on macOS[24].

Xen® [n]

Mitigations for Xen are in development [25]. No mitigation is currently available for CVE-2017-5753 (bounds check bypass). No mitigation is currently available for CVE-2017-5715 (branch target injection), but a patch is being developed. Run guests in HVM or PVH mode to mitigate CVE-2017-5754 (rogue data cache load).

APPLICABILITY

This Advisory is issued under the authority defined in National Security Directive 42[26] and applies to all Executive Departments and Agencies, and to all U.S. Government contractors and agents who operate or use National Security Systems (NSS) as defined in CNSS 4009[27].

DISCLAIMER OF ENDORSEMENT

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

[19] Site Isolation. http://www.chromium.org/Home/chromium-security/site-isolation

[20] Increase security with site isolation. https://support.google.com/chrome/answer/7623121

[21] Chrome Policies. https://www.chromium.org/administrators/policy-list-3#SitePerProcess

[22] Chrome Policy Templates. https://dl.google.com/dl/edgedl/chrome/policy/policy_templates.zip

[23] Mitigations landing for new class of timing attack. https://blog.mozilla.org/security/2018/01/03/mitigations-landing-new-class-timing-attack/

[24] VMSA-2018-0002 VMware ESXi, Workstation and Fusion updates address side-channel analysis due to speculative execution. https://www.vmware.com/us/security/advisories/VMSA-2018-0002.html

[25] Xen XSA-254. https://xenbits.xen.org/xsa/advisory-254.html

[26] National Security Directive 42, “National Policy for the Security of National Security Telecommunications and Information Systems,” dated July 5, 1990.

[27] CNSS Instruction No. 4009, “National Information Assurance Glossary,” dated April 6, 2015.

CONTACT INFORMATION

For further information about this product, please contact:

Client Requirements or General Cybersecurity Inquiries
Cybersecurity Requirements Center
410-854-4200
Email: Cybersecurity_Requests@nsa.gov

TRADEMARK INFORMATION

a. Intel is a registered trademark of Intel Corporation
b. AMD is a registered trademark of Advanced Micro Devices, Inc.
c. ARM is a registered trademark of Arm Limited Soft Bank Group
d. Microsoft is a registered trademark of Microsoft Corp.
e. Linux is a registered trademark of Linux Torvolds
f. macOS is a trademark of Apple, Inc.
g. Android is a trademark of Google, Inc.
h. Chrome OS is a trademark of Google, Inc.
i. Microsoft Edge is a trademark of Microsoft Corp.
j. Internet Explorer is a trademark of Microsoft Corp.
k. Chrome is a trademark of Google, Inc.
l. Firefox is a registered trademark of the Mozilla Foundation
m. VMware is a registered trademark of VMware, Inc.
n. Xen is a registered trademark of Citrix