NATIONAL SECURITY AGENCY
CYBERSECURITY ADVISORY

UPDATED GUIDANCE FOR VULNERABILITIES AFFECTING MODERN PROCESSORS

DISCUSSION

Multiple side-channel vulnerabilities affect Intel®[1], AMD®[2], ARM®[3], and IBM®[4] processors. These vulnerabilities exploit weaknesses in speculative execution to leak unauthorized information. Account permissions, virtualization boundaries, and protected memory regions may be bypassed via exploitation. Multiple CVE®[5]s have been released for side-channel vulnerabilities carrying names like Spectre, Meltdown, and Foreshadow. Vendors have released patches to mitigate vulnerabilities. Vulnerable processors are present in several generations of systems widely deployed within National Security Systems including DoD networks.

MITIGATION ACTIONS

In order to better respond to the continued pace of discovery and development of related vulnerabilities, the following websites should be used as the most current source of vulnerability and mitigation information:

- https://github.com/nsacyber/Hardware-and-Firmware-Security-Guidance
- https://www.us-cert.gov/ncas/alerts/TA18-004A

In general, however, the following mitigations apply to affected systems:

1) Apply system UEFI/BIOS firmware updates provided by system vendors. Firmware updates may not be delivered through established patching services and may be easily missed. Consult vendor support sources, such as Dell®[6] or HP®[7] or similar, for each specific make and model of system.

2) Apply microcode updates provided by system vendors and operating system update services. Microcode updates may have a firmware component update in addition to an operating system kernel update. Follow system vendor guidance for applying firmware updates. Consult operating system vendor security bulletins for software patches.

3) Apply all vendor operating system, driver, and application patches. Perform configuration changes as indicated. Apple®[8], Google®[9], Linux distributions[10], and Microsoft®[11] have released information and updates for the respective operating systems. Web browsers, drivers, software applications, virtualization solutions, and development kits are also affected. Apply all patches. Flaws and unintentional side effects found in initial patch releases have been resolved. Some patches may require configuration changes to enable the full benefit of mitigations. Check vendor configuration guides.

---

1 Addressing Hardware Vulnerabilities https://www.intel.com/content/www/us/en/architecture-and-technology/facts-about-side-channel-analysis-and-intel-products.html . Intel is a registered trademark of Intel Corporation
2 AMD Processor Security https://www.amd.com/en/corporate/security-updates . AMD is a registered trademark of Advanced Micro Devices, Inc.
3 Cache Speculation Issues Update https://developer.arm.com/support/arm-security-updates/speculative-processor-vulnerability/latest-updates/cache-speculation-issues-update . ARM is a registered trademark of ARM Limited
4 IBM Security Bulletins https://www-01.ibm.com/support/docview.wss?uid=nas8N1022433 . IBM is a registered trademark of International Business Machines Corporation
5 CVE is a registered trademark of The MITRE Corporation
6 Dell Support: Microprocessor Side-Channel Vulnerabilities https://www.dell.com/support/meltdown-spectre . Dell is a registered trademark of Dell, Inc.
7 HP Security Bulletin: Side-Channel Analysis Method https://support.hp.com/us-en/document/c05869091 . HP is a registered trademark of Hewlett Packard Corporation
8 About speculative execution vulnerabilities in ARM-based and Intel CPUs https://support.apple.com/en-us/HT208394 . Apple is a registered trademark of Apple, Inc.
9 Meltdown/Spectre vulnerability status for Chrome OS devices https://www.chromium.org/chromium-os/meltdown-spectre-vulnerability-status . Google is a registered trademark of Google, Inc.
10 Meltdown & Spectre – Kernel Side-Channel Attacks – CVE-2017-5754 CVE-2017-5753 CVE-2017-5715 https://access.redhat.com/security/vulnerabilities/speculativeexecution . Linux is a registered trademark of Linus Torvalds
11 Protect your Windows devices against Spectre and Meltdown https://support.microsoft.com/en-us/help/4073757/protect-your-windows-devices-against-spectre-meltdown . Microsoft is a registered trademark of Microsoft Corp.

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.

CONTACT

Cybersecurity Requirements Center
410-854-4200
Cybersecurity_Requests@nsa.gov