UPDATED GUIDANCE FOR VULNERABILITIES AFFECTING MODERN PROCESSORS

DISCUSSION

Multiple side-channel vulnerabilities affect Intel\textsuperscript{[8,9]}, AMD\textsuperscript{[8,9]}, ARM\textsuperscript{[3,6]}, and IBM\textsuperscript{[4,6]} 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 CVEs\textsuperscript{[5,6,7,8]} 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://www.us-cert.gov/ncas/alerts/TA18-004A](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\textsuperscript{[6,8]} or HP\textsuperscript{[7,8]} 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\textsuperscript{[10]}, Google\textsuperscript{[11]}, Linux distributions\textsuperscript{[10]}, and Microsoft\textsuperscript{[8,11]} 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.

---

5. CVE is a registered trademark of The MITRE Corporation.
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