NATIONAL SECURITY AGENCY
CYBERSECURITY ADVISORY

GUIDANCE FOR VULNERABILITIES AFFECTING MODERN PROCESSORS (UPDATE 2)

DISCUSSION

A new set of side-channel vulnerabilities focusing on Intel® processors[1] has been disclosed to the public. These vulnerabilities exploit weaknesses in processor buffers to leak unauthorized information. Vulnerable buffers move data to and from caches affected by previous side-channel vulnerabilities. Account permissions, virtualization boundaries, and protected memory regions may be bypassed via exploitation. The new vulnerabilities are identified as:

- Microarchitectural Data Sampling (MDS)[1] – a generic term encompassing multiple vulnerabilities
- Fallout[2]
- Rogue In-Flight Data Load (RIDL)[2]
- ZombieLoad[3]

Vulnerable processors are present in several generations of systems widely deployed within National Security Systems including DoD networks. Desktops, servers, notebooks, tablets, thin clients, and other computing products are affected. Assume **ALL**[4] Intel® x86 architecture processors are affected – including products with hardware "in-silicon" Spectre and Meltdown mitigations. **Spectre and Meltdown patches are not sufficient to address MDS vulnerabilities.**

MITIGATION ACTIONS

1) Apply system UEFI/BIOS firmware updates provided by system vendors. Firmware updates may include a processor microcode update element. Ensure that the entire firmware update process runs uninterrupted – some implementations have multiple phases. Some firmware updates may not be delivered through widely used patching services. Always check with system vendors, such as Dell® [5] and HP® [6] and similar, for each specific make and model of system. Patch delivery mechanisms may not be consistent across product lines and form factors.

2) Apply all operating system, driver, application, and development library patches. Perform configuration changes as indicated. Xen Project® [7], VMware® [8], Microsoft® [9], Red Hat® [10], Google® [11], Citrix® [12], Apple® [13], and others have released information and updates for their respective products. Additional applications, such as web browsers and document readers, may also require patching. Software development tool updates may contain new instructions and subroutines to mitigate MDS.

---

[1] Deep Dive: Intel Analysis of Microarchitectural Data Sampling https://software.intel.com/security-software-guidance/insights/deep-dive/intel-analysis-microarchitectural-data-sampling

[2] RIDL and Fallout: MDS attacks https://mdsattacks.com

[3] ZombieLoad Attack https://zombieloadattack.com

[4] Deep Dive: CPUID Enumeration and Architectural MSRs https://software.intel.com/security-software-guidance/insights/deep-dive-cpuid-enumeration-and-architectural-msrs

[5] Dell EMC Server Security Notice https://www.dell.com/support/article/us/en/04/sln317156/dell-emc-server-security-notice-for-intel-sa-00233

[6] HPE Products Using Certain Intel Processors, MDS https://support.hpe.com/hpsc/doc/public/display?docLocale=en-US&docid=emr_na-hpesbhf03933en_us

[7] Xen Security Advisory XSA-297 https://xenbits.xen.org/xsa/advisory-297.html

[8] Implementing Hypervisor-Specific Mitigations for MDS Vulnerabilities https://kb.vmware.com/s/article/67577

[9] Microsoft Guidance to Mitigate MDS Vulnerabilities https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/ADV190013

[10] MDS Advisory https://access.redhat.com/security/vulnerabilities/mds

[11] Product Status: MDS https://support.google.com/faqs/answer/9330250

[12] MDS Security Issues and Mitigations https://www.citrix.com/blogs/2019/05/14/microarchitectural-data-sampling-security-issues-and-mitigations

[13] Additional Mitigations for Speculative Execution Vulnerabilities https://support.apple.com/en-us/HT210107

3)Temporarily disable Intel® Hyper-Threading Technology (HT Technology) on systems handling sensitive data. Disable HT until MDS mitigation patches are widely deployed. Lag time between disclosure and the deployment of patches is expected. Initial patches may also miss some edge cases. Wait for the full effectiveness of patches to be understood before restoring HT. Some use cases may see significant performance impacts.

RESOURCES

The following websites are updated as new vulnerabilities are discovered and link to extensive vendor resources:

- https://github.com/nsacyber/Hardware-and-Firmware-Security-Guidance
- https://portal.msrc.microsoft.com/en-us-security-guidance/advisory/ADV190013
- https://www.intel.com/content/www/us/en/architecture-and-technology/mds.html

Vulnerabilities covered in this advisory utilize the following identifiers:

- CVE-2019-11091
- CVE-2018-12127
- CVE-2018-12130
- CVE-2018-12126

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

TRADEMARK INFORMATION

- Apple and MacOS are registered trademarks of Apple, Inc.
- Citrix is a registered trademark of Citrix.
- CVE is a registered trademark of The MITRE Corporation.
- Dell, EMC, and Dell EMC are registered trademarks of Dell, Inc.
- Google, Chrome OS, and Chrome are registered trademarks of Google, Inc.
- HP, HPE, and HP Enterprise are registered trademarks of Hewlett-Packard Company.
- Intel, Core, Xeon, and vPro are registered trademarks of Intel Corporation.
- Linux is a registered trademark of Linus Torvalds.
- Microsoft, Windows, Edge, and Internet Explorer are registered trademarks of Microsoft Corporation.
- Red Hat is a registered trademark of Red Hat, Inc.
- Vmware, vSphere, and ESXi are registered trademarks of VMware, Inc.
- Xen Project is a registered trademark of The Linux Foundation.