Meltdown / Spectre vulnerabilities and impact on Amulet Hotkey products

January 10, 2018
Last updated: 06/07/2018 11:00 EST

New security vulnerabilities that can exploit modern processors have been disclosed by security researchers on January 3, 2018. Please read this notice and the relevant advisories carefully to understand the risks and resolution steps that you may need, or may want, to make within your organization.

The flaws named Meltdown and Spectre pose a risk that malicious programs could steal data which is currently processed on the computer. This might include secret keys, passwords, personal information and confidential documents. Most devices and systems may be vulnerable to some extent.

> ***Special note:*** *At this time Amulet Hotkey have not found any evidence that the DXZ zero client and remote workstation card products are affected by these vulnerabilities. See below for more information.*

Amulet Hotkey is working with technology partners to investigate potential impact to our products. This notice will be updated as information becomes available.

Vulnerabilities

Meltdown and Spectre are related side-channel attacks against modern microprocessors that can result in unprivileged code reading data it should not be able to. These attacks require malicious code to be running locally, which would require a valid account or independent compromise of the target device. Multi-user and multi-tenant systems, including virtualized and public/private cloud environments can face the highest risk. Single users systems that do not readily provide a way to execute code locally face a significantly lower risk.

Meltdown: (CVE-2017-5754)

- **CPU mechanism for triggering:** out-of-order execution. Also described as rogue data cache load, memory access permission check performed after kernel memory read
- **Affected platforms:** Intel x86 processors that implement out-of-order execution – any processor since 1995 (other than Itanium and Atom pre-2013). It is not clear if ARM/AMD are affected.
- **Systems affected:** may include desktops, laptops, workstations, cloud computers and any system that uses an x86 processor.
- **Difficulty of successful attack:** Low – the Kernel memory exploit code is mostly universal.

Spectre: (CVE-2017-5715 and CVE-2017-5753)

- **CPU mechanism for triggering:** speculative execution from branch prediction. Also described as bounds check bypass and branch target injection.
- **Affected platforms:** Intel, AMD and ARM that implement branch prediction – all modern processors are potentially vulnerable.
- **Affected systems:** may include smartphones, tablets, desktops, laptops, workstations, cloud computers and any system that uses an affected processor.
- **Difficulty of successful attack:** High – requires tailoring to the software environment of the victim process.

Solution

Amulet Hotkey products can incorporate components, products and technology from partners. We encourage customers to review vendor advisories and take the appropriate actions to mitigate these vulnerabilities. The tables below list some of the partner products used in Amulet Hotkey products and links to some of the vendor guidance.

General vendor guidance:

- **Apply updates.** Operating system, CPU microcode, GPU driver updates, and some software application updates mitigate these attacks.
- **Solution impact:** The attacks target microprocessor optimizations to improve performance and updates to mitigate these attacks may impact performance for some workloads. Per the US-CERT, patching can reduce performance by up to 30%. Intel guidance indicates minimal impact for most customers, but online reports vary depending on the workload. As such, we recommend that you monitor critical systems accordingly.

Table 1: Amulet Hotkey Products and Solution Partners/Components

Products		Technology Partners	Notes
Blade Workstation			
	CoreStation WM640	Dell EMC PE M-series server w/ Dell customized BIOS, Intel Xeon CPUs, NVIDIA/AMD GPUs, Client OS: Windows / Linux, Teradici Tera2 PCoIP Processor(s)	See vendor guidance below. ***Do not use PE M640 BIOS*** - a WM640 BIOS update is available on the Amulet Hotkey resource site WM640 page.
	CoreStation DXM630		See vendor guidance below. ***Do not use PE M630 BIOS*** - a DXM630 BIOS update is available on the Amulet Hotkey resource site DXM630 page.
	CoreStation DXM620, DXM520, DXM420		See vendor guidance below. ***Do not use PE Mx20 BIOS*** - a DXMx20 BIOS update is available on the Amulet Hotkey resource site DXM620 page, DXM520 page, DXM420 page.
	CoreStation DXM710, DXM610		See vendor guidance below. ***Do not use PE Mx10 BIOS*** - a DXMx10 BIOS is under investigation.
	M1000e system components	Dell EMC PE M1000e enclosure components such as blade interconnect, CMC etc.	See vendor guidance below.
Virtual Blade Workstation / Virtual Desktop Servers			
	CoreStation VM640	Dell EMC PE M-series server, Intel Xeon CPUs, NVIDIA/AMD GPUs, VMware vSphere	See vendor guidance below.
	CoreStation VM630		See vendor guidance below.
	CoreStation VFC640	Dell EMC PE FX2 server, Intel Xeon CPUs, NVIDIA/AMD GPUs, VMware vSphere	See vendor guidance below
	M1000e and FX2s system components	Dell EMC PE M1000e or PE FX2s enclosure components such as blade interconnect, CMC etc.	See vendor guidance below.
KVM Extender and Remote Workstation Graphics Cards			
	DMX, DXP4	NVIDIA/AMD GPUs, Teradici Tera2 PCoIP Processor	Tera2 not vulnerable. See GPU vendor guidance below.
KVM Extender and Remote Workstation Cards			
	DXH, DXL	Teradici Tera2 PCoIP Processor	Not vulnerable - see notes below.
	DXR-H4, DXT-H4	Teradici Tera2 PCoIP Processor, Intel Atom, Win10 IoT OS	Tera2 not vulnerable. A DXR-H4/DXT-H4 firmware update is under investigation, will be posted on Amulet Hotkey resource site. See notes below.
DXZ Zero Clients			
	DXZ models, DXR-Z4	Teradici Tera2 PCoIP Processor	Not vulnerable - see notes below.

Table 2: Vendor Guidance Links:

Amazon	https://aws.amazon.com/security/security-bulletins/AWS-2018-013/
AMD	http://www.amd.com/en/corporate/speculative-execution
ARM	https://developer.arm.com/support/security-update
Citrix	https://support.citrix.com/article/CTX231390
CentOS	https://lists.centos.org/pipermail/centos-announce/2018-January/date.html
Dell EMC	http://www.dell.com/../side-channel-vulnerabilities-impact-on-dell-emc-products
Fujitsu	http://support.ts.fujitsu.com/content/SideChannelAnalysisMethod.asp
Intel	https://security-center.intel.com/advisory../ 01/22/2018 new guidance
Leostream	https://leostream..statement-on-the-meltdown-and-spectre-vulnerabilities
Microsoft	https://support.microsoft.com/../speculative-execution-side-channel-vulnerabilities
NVIDIA	https://www.nvidia.com/en-us/product-security/
RedHat	https://access.redhat.com/security/vulnerabilities/speculativeexecution Performance test report: https://access.redhat.com/articles/3307751
SuSe	https://www.suse.com/support/kb/doc/?id=7022512
Teradici	https://techsupport.teradici.com/../kb3250 - Tera2 is not vulnerable per this article
Ubuntu	https://wiki.ubuntu.com/SecurityTeam/KnowledgeBase/SpectreAndMeltdown
VMware	https://www.vmware.com/security/advisories.html

For more information see the US-CERT list of affected vendors.

Amulet Hotkey DXR-H4 / DXT-H4 KVM Extender Hosts

Amulet Hotkey DXR-H4 and DXT-H4 KVM extender host cards incorporate Teradici Tera2 PCoIP processors, Intel Atom processors and Windows 10 IoT operating system. The Tera2 processor is not vulnerable (see below). Intel has confirmed the ATOM processor model used is affected, however, the risk is considered low due to the following:

- These attacks require the execution of malicious code on the target device.
- The ATOM processor is used for internal system control running firmware developed by Amulet Hotkey that is specific for these products. There is no user GUI and the firmware does not provide an option for the installation and execution of user applications.

While the risk is considered low, Amulet Hotkey is working with partners to update the BIOS and OS used with the ATOM processor to mitigate these vulnerabilities. A firmware update is under investigation and will be posted on the on Amulet Hotkey resource site.

Amulet Hotkey Zero Clients and Host Cards

Amulet Hotkey zero client and KVM Extender/Remote Workstation products incorporate Teradici Tera2 PCoIP processors as well as ARM Cortex M3 or M4 processors. ARM have confirmed that the Cortex M3 and M4 are not affected. Teradici have confirmed that the Tera2 processors are not vulnerable.

- Teradici confirmed the MIPS processor models used in Tera2 PCoIP processors are not impacted by the exploitation techniques described in the Meltdown and Spectre vulnerabilities.
- These attacks require the execution of malicious code on the target device.
- Tera2 Processor firmware does not permit the installation or execution of user applications.
- Teradici controls the firmware and a digital signature must be present for the Tera2 to allow a firmware installation (upgrade or downgrade of firmware).

See important note below.

Important note: *while Tera2 zero clients and remote workstation cards are not directly vulnerable, they may be used to connect to host systems, workstations or virtual desktops that may be vulnerable. Those host systems must be protected accordingly.*

External References

- UK NCSC guidance on Meltdown and Spectre
- CERT/CC Vulnerability Note VU#584653
- US-CERT guidance on Meltdown and Spectre
- Google Project Zero blog post

Change History:

Date	Change
01/10/2018	Notice published
01/12/2018	Added CoreStation DXM620, 520, 420, 710, 610. Updated DXMxxx BIOS notes. Added ARM, Fujitsu and Leostream vendor guidance links. Updated Amulet Hotkey Zero Clients and Host Cards with ARM details.
01/24/2018	Updated DXMxxx BIOS notes based on new Intel guidance. Updated DXR-H4 / DXT-H4 guidance. Added link to Intel 01/22/2018 vendor guidance.
6/7/2018	Updated CoreStation WM640, DXM630, DXM620, DXM520 and DXM420 based on release of new BIOS versions. Added CoreStation VFC640 notes. Added M1000e and FX2s system component notes.

Amulet Hotkey | London, +44 (0) 20 7960 2400 | New York, +1 212-269-9300
www.amulethotkey.com | sales@amulethotkey.com