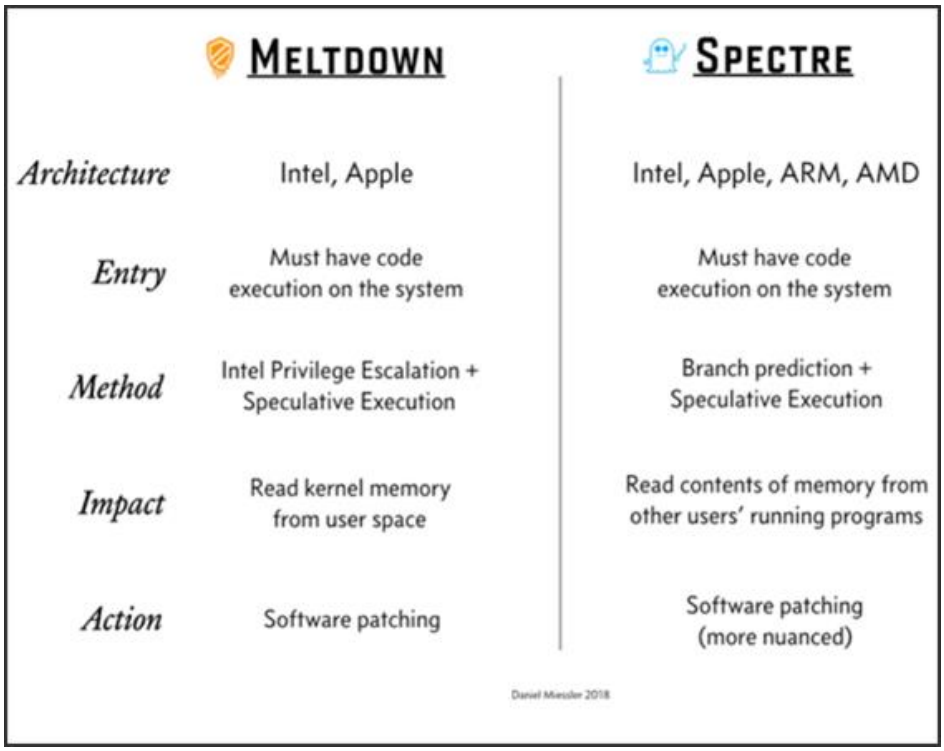
Meltdown and Spectre

Summary of Meltdown & Spectre

The exploits known as Spectre and Meltdown consist of variants listed below and affect the following architectures:



There are many good explanations of these exploits from the industry. More in-depth analysis can be found at the following locations:

- Google Project Zero https://googleprojectzero.blogspot.com/2018/01/reading-privileged-memory-with-side.html
- Stratechery https://stratechery.com/2018/meltdown-spectre-and-the-state-of-technology/
- Rendition Infosec https://www.renditioninfosec.com/2018/01/meltdown-and-spectre-vulnerability-slides/
- Red Hat (High Level) https://www.redhat.com/en/blog/what-are-meltdown-and-spectre-heres-what-you-need-know
- Red Hat (Details) https://access.redhat.com/security/vulnerabilities/speculativeexecution
- CVE-2017-5753
- CVE-2017-5715
- CVE-2017-5754
- https://meltdownattack.com/meltdown.pdf
- https://spectreattack.com/spectre.pdf

Summary of speculative execution variants **Vulnerability**	**CVE**	**Exploit name**	**Public vulnerability name**
Spectre	2017-5753	Variant 1	Bounds Check Bypass (BCB)
Spectre	2017-5715	Variant 2	Branch Target Injection (BTI)
Meltdown	2017-5754	Variant 3	Rogue Data Cache Load (RDCL)
Spectre-NG	2018-3640	Variant 3a	Rogue System Register Read (RSRE)
Spectre-NG	2018-3639	Variant 4	Speculative Store Bypass (SSB)
Spectre-NG	2018-3665		Lazy FP State Restore
Spectre-NG	2018-3693		Bounds Check Bypass Store (BCBS)
Foreshadow	2018-3615	Variant 5	L1 Terminal Fault (L1TF)
Foreshadow-NG	2018-3620		L1 Terminal Fault
Foreshadow-NG	2018-3646		

The following table describes each of the variants and risks.

CVE-2017-5753 (variant #1/Spectre)	A **Bounds-checking** exploit during branching. This issue is fixed with a kernel patch.	Spectre is primarily an issue for processes where chunks of untrusted code are executed within the process. In doing so, the untrusted code can read data from areas it should not normally have access to. The industry guidance is that the risk from Spectre is primarily to web browsers where malicious JavaScript (in an advert for example) can be used to read data from elsewhere in the browsers memory.	Variant #1 protection is always enabled. It is not possible to disable the patches.
CVE-2017-5715 (variant #2/Spectre)	An **indirect branching poisoning** attack that can lead to data leakage. This attack allows for a virtualized guest to read memory from the host system. This issue is corrected with microcode, along with kernel and virtualization updates to both guest and host virtualization software. This vulnerability requires both updated microcode and kernel patches.		Variant #2 behaviour is controlled by the ibrs and ibpb tuneables

CVE-2017-5754 (variant #3/Meltdown)	An exploit that uses **speculative cache loading** to allow a local attacker to be able to read the contents of memory. This issue is corrected with kernel patches.	Meltdown allows an attacker to escape the confines of its Docker Container, VM, or Process and read arbitrary data including that from the kernel. While the risk of infection in a closed systems is low, VIAVI recommends patching against this attack.	Variant #3 behaviour is controlled by the pti tuneable (nopti/pti_enabled)
CVE-2018-3615 (L1TF)	https://access.redhat.com/security/cve/cve-2018-3615	RHEL claims to not be vulnerable	
CVE-2018-3620 (L1TF)	https://access.redhat.com/security/cve/cve-2018-3620	Should update kernel	kernel update only
CVE-2018-3640 (L1TF)	https://access.redhat.com/security/cve/cve-2018-3640	Un-patchable in software... needs microcode update	
CVE-2018-3665 (Lazy FP State Restore)	https://access.redhat.com/security/cve/cve-2018-3665	Theoretical exposure of data in floating point registers	Should set eagerfpu=on on systems with CPUs older than Sandy Bridge

Red Hat has produced a full set of patches that also incorporates the required Intel Microcode changes to mitigate all three variants of Spectre and Meltdown.

The guidance from VIAVI is to apply the RHEL Patch set, Microcode update, and the BIOS changes from DELL. Then reboot the server and verify the system is protected by running the check script from https://www.cyberciti.biz/faq/check-linux-server-for-spectre-meltdown-vulnerability

Given the low level of exposure to on-prem, private network systems to CVE-2017-5715 (variant #2/Spectre), and the significant performance hit that disabling branch prediction in the CPU brings, it is recommended to disable the IBRS change in the kernel for products in this category. This removes the protection for CVE-2017-5715 (variant #2/Spectre) but mitigates the performance impact of the patch. If your IT policy does not allow this, then the performance of the system would need to be resized. Please refer to product specific guidance.

VIAVI continues to investigate a possible alternative solution to mitigating CVE-2017-5715 (variant #2/Spectre) with better performance results using a technique from Google called Retpoline. This technique provides protection from CVE-2017-5715 (variant #2/Spectre) at minimal performance loss. However, Retpoline requires Red Hat to make changes and re-issue their Linux kernel with the modifications. Linux has not yet made the changes and re-issued the kernel.

Please refer to product specific guidance below.

Product Specific Information

NITRO Mobile

- **xSIGHT**

CVE-2017-5753 (variant #1/Spectre)	As xSIGHT is an on-premises system with no interaction with the external internet and no dynamic use of untrusted code from the web, it is not exposed to Spectre in the same manner as a browser	Variant #1 protection is always enabled. It is not possible to disable the patches.	Red Hat's performance testing for variant #1 did not show any measurable impact. That is also reflected in our own testing.
CVE-2017-5715 (variant #2/Spectre)		Variant #2 behaviour is controlled automatically by the latest kernels, it can be manually changed if required.	Update as of the latest OS patches in RHEL for xSIGHT 2.2 and 2.3 we are now fully protected against variant #2/Spectre using the new Retpoline enabled kernel.
CVE-2017-5754 (variant #3/Meltdown)	While the risk of infection in a closed system such as xSIGHT is low, VIAVI recommends patching against this attack.	Variant #3 behavior is controlled by the pti tunable (nopti/pti_enabled)	~2% This is a minor impact and is easily absorbed.

RedHat has produced a full set of patches that also incorporate the required Intel Microcode changes to mitigate all three variants of Spectre and Meltdown in addition to providing a Retpoline enabled kernel to provide protect ion against variant #2/Spectre without the initial performance hit of the original mitigations.

xSIGHT systems running 2.2 and 2.3 on the latest OS patch bundle are fully protected, you can verify this for your customer by using the RHEL Meltdown and Spectre check tool spectre-meltdown--2018-10-05-1354.sh

- **AcceSS7**

CVE-2017-5753 (variant #1/Spectre)		
CVE-2017-5715 (variant #2/Spectre)	As acceSS7 is an on-prem system with no interaction with the external internet and no dynamic use of untrusted code from the web, it is not exposed to Spectre in the same manner as a browser VIAVI currently does not recommend patching the Windows systems because Microsoft does not have a recommended patch currently available.	our lab test shows ipcore CPU usage will increase about 5%, after installing all the kernel and BIOS patches. We would assume other a7 components have the similiar impact.
CVE-2017-5754 (variant #3/Meltdown)	While the risk of infection in a closed system such as acceSS7 is low, VIAVI recommends patching against this attack.	
CVE-2018-3615 (L1TF)	NA to a7	
CVE-2018-3620 (v5 L1TF)	https://www.suse.com/support/kb/doc/?id=7023077 Install the latest Microcode updates from Intel to enable the L1 Data-cache flush features. These are either provided by SUSE in the "ucode-intel" or "microcode_ctl" packages, and/or via your BIOS / System vendor. The CPU microcode releases from Intel for addressing Spectre v4 in the last months already contain this feature. SUSE provides "ucode-intel" and "microcode_ctl" packages containing the Intel provided CPU microcode bundles, and versions 20180703 and newer, also already contain this feature. The CPU flag is shown in /proc/cpuinfo as "flush_l1d" flag when available also need to update kernel based on instructions for SLES11SP4 and SLES12SP3: https://www.suse.com/security/cve/CVE-2018-3620/	
CVE-2018-3640 (v3a L1TF)	Intel will fix this issue solely with CPU Microcode updates, no updates for the Linux Kernel or Hypervisors will be required: https://www.suse.com/security/cve/CVE-2018-3640/	
CVE-2018-3646(L1TF)	NA to a7	
CVE-2018-3665 (Lazy FP State Restore)	https://www.suse.com/support/kb/doc/?id=7023167	

	To address this issue please upgrade to kernel version 3.0.101-108.63 or later	
CVE-2018-3639 (v4)	https://www.suse.com/support/kb/doc/?id=7022937 The mitigating solution is to disable the "Memory Disambiguation" feature in the processor, either system-wide or selectively for single processes. On Intel x86 systems, updated CPU microcode is required to enable this mitigation. This microcode is either supplied by your hardware / BIOS vendor or by SUSE using the official Intel released microcode packages. Note :The minimum required Intel microcode base-level for this mitigation is the Intel 20180807 release (across all versions of SLES).Mitigations need to be implemented for the Linux Kernel and for Hypervisors, both for passing through new CPU flags and MSR registers (on x86) and supporting of switching off/on the mitigation. For the Linux kernel, on both bare metal and virtual machines, it can be enabled / disabled using the kernel boot command line and/or with a thread-specific prctl() system call.	
CVE-2018-3693	SUSE is still working on solution, do not need microcode fixes, https://www.suse.com/support/kb/doc/?id=7023075	

SUSE has produced a full set of patches that also incorporate the required Intel Microcode changes to mitigate all three (v1/v2/v3) variants of Spectre and Meltdown on https://www.suse.com/support/kb/doc/?id=7022512. For all rest variants, the latest microcode and or SUSE kernel need to be installed, see above table for solution for each vulnerability.

Note SUSE only provide patches for SLES11 SP4, hence it's a must for customer to upgrading to SLES11 SP4 before applying these patches.

Please also install the HPE BIOS patch for DL380 G9 from https://support.hpe.com/hpsc/swd/public/detail?sp4ts.oid=1009087943&swItemId=MTX_83a8df74a7f94ea7b66b5c53ce&swEnvOid=4184#tab3

VIAVI recommends applying the SUSE Patch set, Microcode update, and the BIOS changes from HPE. Then reboot the server and verify the system is protected by running the check script from https://www.cyberciti.biz/faq/check-linux-server-for-spectre-meltdown-vulnerability.

- **LI**
    - **GEOperformance**

CVE-2017-5753 (variant #1/Spectre)	GEO is an on-prem system with no interaction with the external internet and no dynamic use of untrusted code from the web. It is not exposed to Spectre in the same manner as a browser.	
CVE-2017-5715 (variant #2/Spectre)	We also need to consider the separate components of GEO. Loading servers running Windows, for both file based and Lightning systems. Application servers running Windows DB servers running Oracle on Linux or Windows VIAVI currently does not recommend patching the Windows systems because Microsoft does not have a recommended patch currently available.	
CVE-2017-5754 (variant #3/Meltdown)	While the risk of infection in a closed system like GEO is low, VIAVI does not recommend patching the Windows systems, as Microsoft do not have a recommended patch at this time.	

Testing of our Windows systems is in progress but is hampered by Microsoft not providing a patch that provides a recommended stable performant version. We are waiting on this patch to complete our testing on Windows 2008, 2012 and 2016.

We are also waiting on a BIOS update from HP for our blade systems to perform full testing of this patch.

We are in the process of testing the Oracle DB on Linux and will update this page as soon as they are available.

NITRO Vision

Updated to apply the latest set of patches. **In short all the patches can be applied - and should be**. The provide a noticeable performance improvement over the previous set of patches. All functionality is maintained with the latest patches.

The operating system supplied by the customer, of image provided by the application, should be updated to include the Reptoline solution.

https://conf1.ds.jdsu.net/wiki/pages/viewpage.action?pageId=62003142

Observer

To install vulnerability mitigations on GigaStor and Apex systems (G3+ - W2012r2), execute the following steps:

1. Download and update the BIOS and firmware for the SuperMicro motherboard in the system.
2. Download and install MS KB4338824 (windows8.1-kb4338824-x64_2718920716ec19174fcfa4a43ab5bbe40a27a732).
3. Reboot the system.
4. Download SpeculationControl.psd1 powershell-based vulnerability checker, and run from powershell.

KB4338824 contains mitigations for the following Spectre and Meltdown variants:

- CVE-2017-5715 (Spectre Variant 2) – "Branch Target Injection" (Disabled by default)
- CVE-2017-5753 – "Bounds Check Bypass" (Enabled by default, no option to disable)
- CVE-2017-5754 (Meltdown) – "Rogue Data Cache Load" (Disabled by default)
- CVE-2018-3639 – “Speculative Store Bypass” (Disabled by default)

To enable mitigations for 3639, 5715 and 5754:

reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management" /v FeatureSettingsOverride /t REG_DWORD /d **8** /f

reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management" /v FeatureSettingsOverrideMask /t REG_DWORD /d 3 /f

reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Virtualization" /v MinVmVersionForCpuBasedMitigations /t REG_SZ /d "1.0" /f

CVE-2017-5753 (variant #1/Spectre)	Observer Suite (including Analyzer, GigaStor, Apex, and Management Server) is an on-prem system with no interaction with the external internet and no dynamic use of untrusted code from the web. It is not exposed to Spectre in the same manner as a browser. VIAVI currently does not recommend patching the Windows systems because Microsoft does not have a recommended patch available.		No performance impact has been measured.
CVE-2017-5715 (variant #2/Spectre)			No performance impact has been measured.

CVE-2017-5754 (variant #3/Meltdown)	While the risk of infection in a closed system such as Observer is low, VIAVI does not recommend patching the Windows systems because Microsoft does not have a recommended patch available.		No performance impact has been measured.

ObserverLIVE

There is no impact to our customers on ObserverLIVE. https://aws.amazon.com/security/security-bulletins/AWS-2018-013/

Fusion

All meltdown and spectre patches can be applied and there is no performance impact.

CVE-2017-5753 (variant #1/Spectre)	Fusion is an on-prem system with no interaction with the external internet and no dynamic use of untrusted code from the web. It is not exposed to Spectre in the same manner as a browser.	Variant #1 protection is always enabled. It is not possible to disable the patches	No performance impact has been measured.
CVE-2017-5715 (variant #2/Spectre)		Variant #2 behaviour is controlled by the ibrs and ibpb tuneable	No performance impact has been measured.
CVE-2017-5754 (variant #3/Meltdown)	The Fusion components are typically deployed as virtual guests within a customer managed host environment. While the risk of infection from Fusion is low, Viavi recommends patching the host systems against this attack and will be updating Fusion's guest OS usage in a future release.	Variant #3 behaviour is controlled by the pti tuneable (nopti/pti_enabled)	No performance impact has been measured.

EtherAssure

All meltdown and spectre patches can be applied and there is no performance impact.

CVE-2017-5753 (variant #1/Spectre)	EtherASSURE (including the NetComplete servers, QT600 and JMEP probes, and the ESAM mediation server) is an on-prem system with no interaction with the external internet and no dynamic use of untrusted code from the we. It is not exposed to Spectre in the same manner as a browser.	Variant #1 protection is always enabled. It is not possible to disable the patches	No performance impact has been measured.
CVE-2017-5715 (variant #2/Spectre)		Variant #2 behavior is controlled by the ibrs and ibpb tunables	No performance impact has been measured.
CVE-2017-5754 (variant #3/Meltdown)	While the risk of infection in a closed system such as EtherASSURE is low, Viavi recommends patching against this attack.	Variant #3 behavior is controlled by the pti tunable (nopti/pti_enabled)	No performance impact has been measured.