VIAVI

Meltdown & Spectre Vulnerability Impacts on VIAVI Products

January 2018

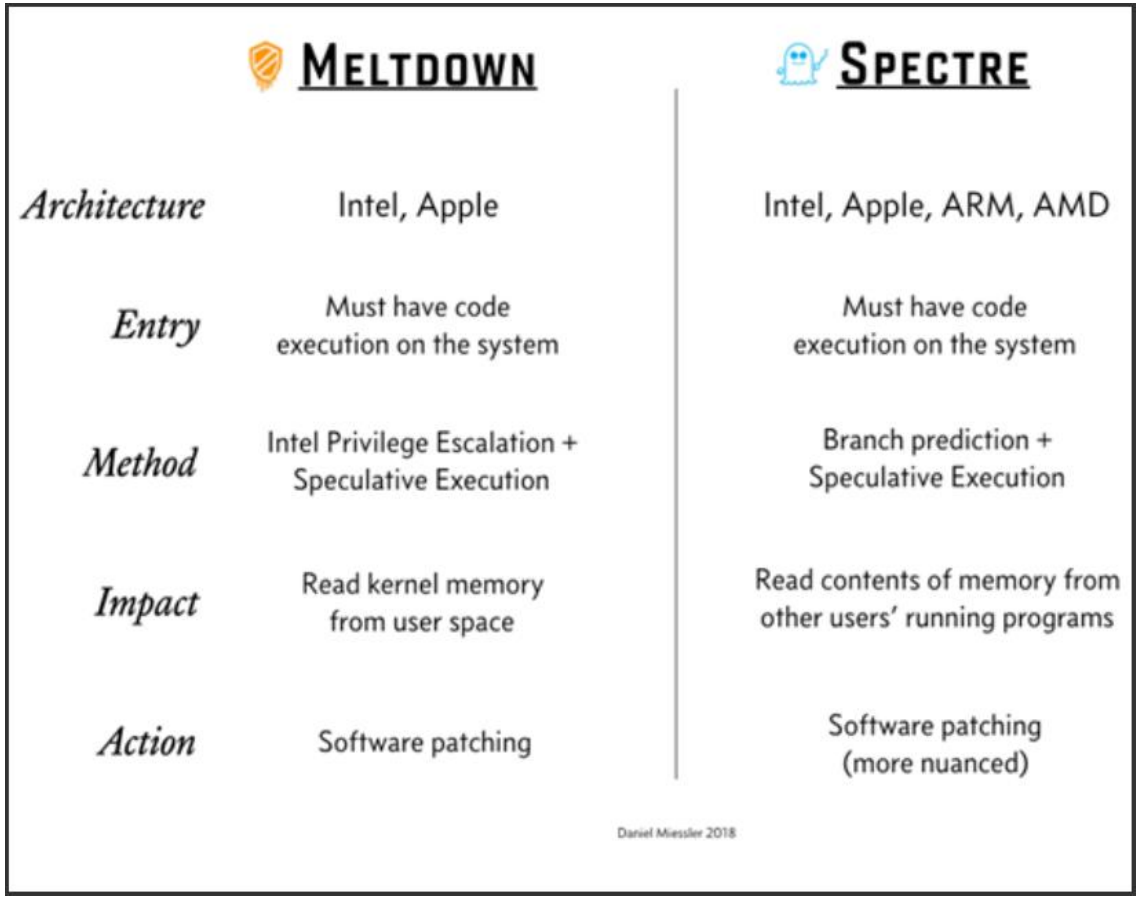
Vulnerabilities - Industry Information

Basic synopsis of the vulnerabilities:

- Both attacks assume an “an attacker program” to be installed and running on the target.

References:

- Meltdown
  - CVE-2017-5753
  - CVE-2017-5715
  - https://meltdownattack.com/meltdown.pdf
- Spectre
  - CVE-2017-5754
  - https://spectreattack.com/spectre.pdf



	MELTDOWN	SPECTRE
Architecture	Intel, Apple	Intel, Apple, ARM, AMD
Entry	Must have code execution on the system	Must have code execution on the system
Method	Intel Privilege Escalation + Speculative Execution	Branch prediction + Speculative Execution
Impact	Read kernel memory from user space	Read contents of memory from other users’ running programs
Action	Software patching	Software patching (more nuanced)

Daniel Miessler 2018

VIAVI Product Categorization & Security Impact

“Unaffected Processor” VIAVI Products

- The product processor cannot be a target of this attack (based on industry information)

Impact: None

“**“Closed System”** VIAVI Products

- VIAVI SW running on VIAVI HW
- Installing external programs on VIAVI equipment is not allowed or supported. The only SW installed/running is VIAVI SW.

Impact: None

“**Open System**” VIAVI Products

- VIAVI SW running on VIAVI HW
- Customer may have access to a controlled login account.
- Customer may be allowed to install external programs on VIAVI equipment
- Automatic installation of programs onto VIAVI equipment may be possible (e.g. webscript run in a browser)

Impact: Potential

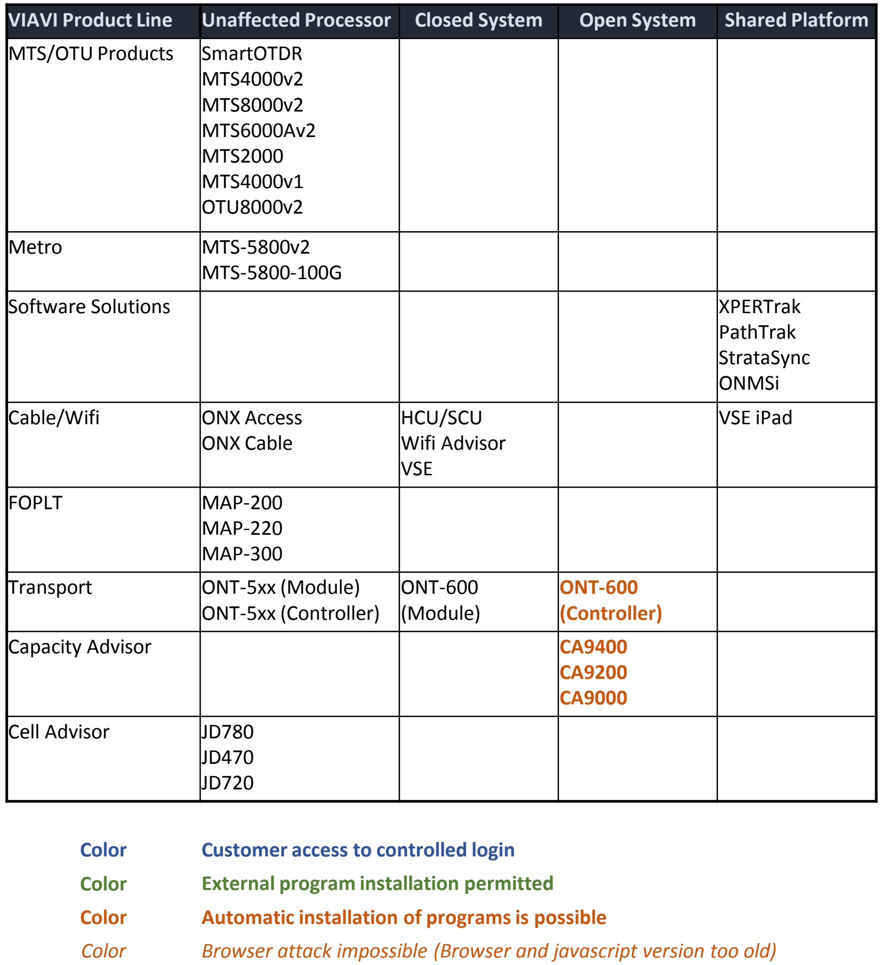
“**Shared Platform**” VIAVI Products

- VIAVI software running on a 3rd party platform, e.g. on a Microsoft Windows Server operating system
- The 3rd party platform can co-host customer and/or 3rd party software.

Impact: Yes

See detailed per product analysis in the slides attached to this package.

VIAVI Product Impact - Meltdown



VIAVI Product Line	Unaffected Processor	Closed System	Open System	Shared Platform
MTS/OTU Products	SmartOTDR MTS4000v2 MTS8000v2 MTS6000Av2 MTS2000 MTS4000v1 OTU8000v2			
Metro	MTS-5800v2 MTS-5800-100G			
Software Solutions				XPERTrak PathTrak StrataSync ONMSi
Cable/Wifi	ONX Access ONX Cable	HCU/SCU Wifi Advisor VSE		VSE iPad
FOPLT	MAP-200 MAP-220 MAP-300			
Transport	ONT-5xx (Module) ONT-5xx (Controller)	ONT-600 (Module)	**ONT-600 (Controller)**	
Capacity Advisor			**CA9400 CA9200 CA9000**	
Cell Advisor	JD780 JD470 JD720			

Color	**Customer access to controlled login**
Color	**External program installation permitted**
Color	**Automatic installation of programs is possible**
Color	*Browser attack impossible (Browser and javascript version too old)*

VIAVI Product Impact - Spectre

VIAVI Product Line	Unaffected Processor	Closed System	Open System	Shared Platform
MTS/OTU Products		SmartOTDR MTS4000v2 *MTS8000v2* *MTS6000Av2* *MTS2000* *MTS4000v1* OTU8000v2		
Metro		**MTS-5800v2** **MTS-5800-100G**		
Software Solutions				XPERTrak PathTrak StrataSync ONMSi
Cable/Wifi		ONX Access ONX Cable HCU/SCU Wifi Advisor VSE		VSE iPad
FOPLT		MAP-200 MAP-220 MAP-300		
Transport	ONT-5xx (Module) ONT-5xx (Controller)	ONT-600 (Module)	**ONT-600 (Controller)**	
Capacity Advisor			**CA9400** **CA9200** **CA9000**	
Cell Advisor		JD780 JD470 JD720		

Color	**Customer access to controlled login**
Color	**External program installation permitted**
Color	**Automatic installation of programs through browser is possible**
Color	*Browser attack impossible (Browser and javascript version too old)*

General Note: Mobile Apps

Vulnerability mitigation requires platform specific patches

- Apple
    - iOS patches (11.2 and 11.2.2) are available to address the issues
- Android
    - Patches are in place for newer products.
    - Legacy products (old phones or tablets) may still contain an issue if SW updates are no longer supported

VIAVI Product Vulnerability Technical Analysis

Product Line: Capacity Advisor

Response to Meltdown: Exposure very Low

- The Capacity Advisor 9400/9200/9000 are systems running on Intel processors. Capacity Advisor is deployed in trusted customer lab environments behind customer firewalls. This environment normally does not allow any access to the Internet. The only secret information in the system are authentication keys (e.g. permanent K, OP, and some dynamic key CK, IK). All security information on the USIM is installed by the operator and is not accessible by the subscriber and the keys are only used for test purposes. No external code can be run on Capacity Advisor. There are no means for attackers to deploy native malware applications on the system. The only possible means would be a javascript injection from the browser. Administrator can gain access to the browser but customers cannot do this and VIAVI personnel is never supposed to use it.
- **Source**: Meltdown Vulnerability Abstract - https://meltdownattack.com/meltdown.pdf

Response to Spectre: Exposure very Low

- The Capacity Advisor 9400/9200/9000 are systems running on Intel processors. Capacity Advisor is deployed in trusted customer lab environments behind customer firewalls. This environment normally does not allow any access to the Internet. The only secret information in the system are authentication keys (e.g. permanent K, OP, and some dynamic key CK, IK), as well as the AKA algorithms. All security information on the USIM is installed by the operator and is not accessible by the subscriber and the keys are only used for test purposes. No external code can be run on Capacity Advisor. There are no means for attackers to deploy native malware applications on the system. The only possible means would be a javascript injection from the browser. Administrator can gain access to the browser but customers cannot do this and VIAVI personnel is never supposed to use it.
- **Sources**: Spectre Vulnerability Abstract - https://spectreattack.com/spectre.pdf, https://developer.arm.com/support/security-update

Product Line: Transport

Response to Meltdown: Exposure very Low

- ONT-5xx: unaffected processor.
- The ONT-600 product family uses Intel processors which are potentially vulnerable.
- ONT-600 modules are ‘closed systems’. There are no means to deploy native malware applications on the system.
- ONT-600 high end controllers allow to deploy additional software. ONT-600 is deployed in trusted customer lab environments. The only secret information in the system are authentication keys for module access.
- **Source**: Meltdown Vulnerability Abstract - https://meltdownattack.com/meltdown.pdf

Response to Spectre: Exposure very Low

- ONT-5xx: unaffected processor
- ONT-600 modules are ‘closed systems’. There are no means to deploy native malware applications on the system.
- ONT-600 high end controllers allow to deploy additional software. ONT-600 is deployed in trusted customer lab environments. The only secret information in the system are authentication keys for module access.
- **Sources**: Spectre Vulnerability Abstract - https://spectreattack.com/spectre.pdf, https://developer.arm.com/support/security-update

Product Line: Software Solutions

XPERTrak: Yes, vulnerable

- Servers running XPERTrak and PathTrak are vulnerable to this class of attack since they are installed on Microsoft Windows Server operating systems, including Windows Server 2008 R2, Windows Server 2012 R2, or Windows Server 2016.
- **Resolution:**
  - Microsoft has provided the following guidance to protect against this class of vulnerabilities.
  - https://support.microsoft.com/en-us/help/4072698/windows-server-guidance-to-protect-against-the-speculative-execution
  - Please refer to this guidance. VIAVI recommends you follow the recommendations from Microsoft and their hardware and virtual ware vendors.

StrataSync: Yes, vulnerable à Closed

- Servers running StrataSync on Amazon AWS are vulnerable to this class of attack.
- **Resolution:**
  - AWS has made patches available https://aws.amazon.com/security/security-bulletins/AWS-2018-013/ for this class of vulnerabilities.
  - We are planning to apply these patches this Friday 01/12/2018 at 8:00PM. These patches require system reboot and we'll send out a notification to StrataSync system admins.

ONMSi: Yes, vulnerable

- Servers running ONMSi are vulnerable to this class of attack since they are installed on Microsoft Windows Server operating systems, including Windows Server 2008 R2 and Windows Server 2012 R2.
- **Resolution:**
  - Microsoft has provided the following guidance to protect against this class of vulnerabilities.
  - https://support.microsoft.com/en-us/help/4072698/windows-server-guidance-to-protect-against-the-speculative-execution
  - Please refer to this guidance. VIAVI recommends you follow the recommendations from Microsoft and their hardware and virtual ware vendors.

Product Line: Cable/Wifi

ONX, Wifi Advisor, VSE and HCU/SCU

- Both Meltdown and Spectre are local attacks that require executing malicious software on the systems.
- A user without appropriate credentials cannot install malicious software on the ONX, VSE and HCU/SCU.
- Lack of privileged execution prevents revealing of restricted memory contents.
- These are individual devices which by default have a lower practical risk.
- iPad associated with the VSE however need to be upgraded (as Apple has released patches).

Product Line: Metro & FTS

SmartOTDR & MTS4000v2
The SmartOTDR and MTS4000v2 are embedded instruments running on ARM processors (Cortex A9 core).

- **Meltdown**: they are unaffected by the Meltdown issue: **no threat**.
- **Spectre**: the hardware is vulnerable to Spectre exploit. However, this is a closed embedded Linux system which operates independently and unconnected in normal operation. “It is important to note that this method is dependent on malware running locally” (source: ARM security update). There are no means for attackers to deploy native malware applications on the test instrument. Moreover there is no web browser in these products, this prevents Javascript injection from the browser: **no exposure**.

- Source: https://developer.arm.com/support/security-update

MTS8000v2, MTS6000Av2, MTS2000, MTS4000v1
These are embedded instruments running on PowerPC processor (440 & 465 cores)

- **Meltdown**: with current knowledge’s they are unaffected by the Meltdown issue: **no threat**.
- **Spectre**: the hardware **could** be vulnerable to Spectre exploit, not confirmed with current knowledge’s. However, this is a closed embedded Linux system which operates independently and unconnected in normal operation. About possibility of Javascript injection from the browser, Javascript version used in web browser of these instruments has not the capability of precise timing measurements. Knowing that this new class of attacks involves measuring precise time intervals : **no exposure**

- Source: https://www.mozilla.org/en-US/security/advisories/mfsa2018-01/

OTU8000v2
This is an embedded rack mounted instrument running on PowerPC processor (440 core)

- **Meltdown**: with current knowledge’s it is unaffected by the Meltdown issue: **no threat**.
- **Spectre**: the hardware **could** be vulnerable to Spectre exploit, not confirmed with current knowledge’s. However, this is a closed embedded Linux system. There is no web browser in this product, this prevents Javascript injection from the browser: **no exposure**

Product Line: Metro & FTS

MTS-5800v2, MTS-5800-100G
These are embedded instruments running on an ARM processor.

- **Meltdown**: They are unaffected by the Meltdown issue: **No Threat**.
- **Spectre**:   the hardware is vulnerable to the exploit. However, this is a closed embedded linux system which operates independently and unconnected in normal operation. "It is important to note that this method is dependent on malware running locally" (source: ARM security update). There are no means for attackers to deploy native malware applications on the test instrument. The only possible means would be a javascript injection from the browser. In the event of the exploit, it is unlikely that there would be confidential business information on the instrument unless placed there and viewed in a file browser. The web browser is not required for device operation.

- **Source**: Meltdown Vulnerability Abstract - https://meltdownattack.com/meltdown.pdf
- **Sources**: Spectre Vulnerability Abstract - https://spectreattack.com/spectre.pdf, https://developer.arm.com/support/security-update
- **Recommendation**: Monitor patch options as apply in future release

Product Line: FOPLT

MAP-200
The MAP-200 platform is an embedded instrument running on a PowerPC 440EPX.

- **Meltdown**: **No Threat.** Power PC is not identified as a vulnerable processor
- **Spectre**: **No Exposure.**
  - The hardware **could** be vulnerable to Spectre, but no exploit has been confirmed. Spectre is a side-channel attack which requires the exploit code to run on the same processor. However, this is a closed embedded Linux system. Javascript has not been enabled in the embedded web browser so it is not further vulnerable to code-injection attacks through this vector.

MAP-220
The MAP-200 platform is an embedded instrument running on a ARM Cortex A8.

- **Meltdown**: **No Threat.** ARM is not identified as a vulnerable processor
- **Spectre**: **No Exposure.**
  - The ARM processor is vulnerable, however there is no capability to exploit. Spectre is a side-channel attack which requires the exploit code to run on the same processor. However, this is a closed embedded Linux system. There is no web browser support to allow for code-injection attack through this vector.

MAP-300 (under development)
The MAP-300 platform is an embedded instrument running on a ARM Cortex A15.

- **Meltdown**: **No Threat.** ARM is not identified as a vulnerable processor
- **Spectre**: **No Exposure.**
  - The MAP-300 is under development and there are no fielded units.

Product Line: CellAdvisor

JD780, 740, 720
These are embedded instruments running on an ARM processor.

- **Meltdown**: They are unaffected by the Meltdown issue: **No Threat**.
- **Spectre**: **No exposure**
  CellAdvisor products need to patch and some architecture review for future release. However, they could not install/run malware applications on the system because those are operated independently and unconnected in normal operation.