Security Notification – Spectre and Meltdown V2.1

5-Jan-2018 (Updated on 6-Feb-2018)

Overview

Schneider Electric has become aware of two side channel attacks that leverage critical vulnerabilities in a wide range of computer CPU. These vulnerabilities have been named Spectre and Meltdown. Spectre tricks other applications into accessing arbitrary locations in their memory. Meltdown breaks the mechanism that keeps applications from accessing arbitrary system memory. There have been no known exploits in the wild. Schneider is actively assessing the impact on our offers.

Details

Meltdown:

Desktop, Laptop, and Cloud computers may be affected by Meltdown. Every Intel processor which implements out-of-order execution is potentially affected, which is effectively every processor since 1995 (except Intel Itanium and Intel Atom before 2013). Researchers have successfully tested Meltdown on Intel processor generations released as early as 2011. Currently, researchers have only verified Meltdown on Intel processors.

CVE-2017-5754 is the official vulnerability reference to Meltdown.

Spectre:

Desktops, Laptops, Cloud Servers, as well as Smartphones may be affected by Spectre. All modern processors capable of keeping many instructions in flight are potentially vulnerable. Researchers have verified Spectre on Intel, AMD, and ARM processors. However, in a statement AMD said there is nearly no risk to their products.

CVE-2017-5753 and CVE-2017-5715 are the official vulnerability references to Spectre.

For Schneider Electric Product Specific Information regarding Spectre and Meltdown Impact, Please go here: https://www.schneider-electric.com/en/download/document/SEVD-2018-010-01/

Recommended Mitigations

Schneider Electric is actively monitoring vendor research into these vulnerabilities to determine appropriate actions to be taken. At the time of this publication, information is being updated rapidly and the impact of proposed mitigations and patches remains unclear. Many of the initial mitigations proposed by hardware and operating system vendors indicate a high level of potential performance impact, Schneider Electric recommends caution if mitigations or patches are applied to critical and/or performance constrained systems. If you elect to apply recommended patches or mitigations in advance of further guidance from Schneider Electric, we strongly recommend evaluating the impact of those measures on a Test & Development environment or an offline infrastructure.

- Microsoft: Please refer to Microsoft support sites for further information.
  - https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV180002
  - https://support.microsoft.com/en-us/help/4073119/windows-client-guidance-for-it-pros-to-protect-against-speculative-exe
  - https://support.microsoft.com/en-us/help/4072698/windows-server-guidance-to-protect-against-the-speculative-execution
- Linux: Kernel page table isolation (KPTI), a hardening technique designed to improve security by isolating the kernel space from user space memory has already been implemented in the Linux kernel. Please visit your respective Linux distribution site for patches.
- Cloud: Amazon Web Services and Microsoft Azure are expected to apply patches on 4 January 2018 to address mitigations for these attacks.

We strongly recommend following industry cybersecurity best practices such as:

- Locate control and safety system networks and remote devices behind firewalls, and isolate them from the business network.
- Physical controls should be in place so that no unauthorized person would have access to the ICS and safety controllers, peripheral equipment or the ICS and safety networks.
- All controllers should reside in locked cabinets and never be left in the “Program” mode.
- All programming software should be kept in locked cabinets and should never be connected to any network other than the network for the devices that it is intended.
- All methods of mobile data exchange with the isolated network such as CDs, USB drives, etc. should be scanned before use in the terminals or any node connected to these networks.
- Laptops that have connected to any other network besides the intended network should never be allowed to connect to the safety or control networks without proper sanitation.
- Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet.
  When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPNs may have vulnerabilities and should be updated to the

most current version available. Also recognize that VPN is only as secure as the connected devices.

Additional Guidance in Appendix A

For More Information

Meltdown and Spectre Official site: https://meltdownattack.com/

Microsoft OS: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV180002

Linux based fix : https://gruss.cc/files/kaiser.pdf

KAISER: https://lwn.net/Articles/738975/

AMD statement: https://www.cnbc.com/2018/01/03/amd-rebukes-intel-says-flaw-poses-near-zero-risk-to-its-chips.html

Reading privileged memory with a side-channel- Google Project Zero Blog post: https://googleprojectzero.blogspot.co.at/2018/01/reading-privileged-memory-with-side.html

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

Google: https://support.google.com/faqs/answer/7622138

If you require additional support, Schneider Electric Industrial Cybersecurity Services team are available to help. Please visit: https://www.schneider-electric.com/en/work/services/field-services/industrial-automation/industrial-cybersecurity/industrial-cybersecurity.jsp

To obtain full details on the issues and assistance on how to protect your installation, please contact your local Schneider Electric representative. These organizations will be fully aware of the situation and can support you through the process.

For further information on vulnerabilities in Schneider Electric's products, please visit Schneider Electric's cybersecurity web page at http://www2.schneider-electric.com/sites/corporate/en/support/cybersecurity/cybersecurity.page

About Schneider Electric
Schneider Electric is leading the Digital Transformation of Energy Management and Automation in Homes, Buildings, Data Centers, Infrastructure and Industries.

With global presence in over 100 countries, Schneider is the undisputable leader in Power Management – Medium Voltage, Low Voltage and Secure Power, and in Automation Systems. We provide integrated efficiency solutions, combining energy, automation and software.

In our global Ecosystem, we collaborate with the largest Partner, Integrator and Developer Community on our Open Platform to deliver real-time control and operational efficiency.

We believe that great people and partners make Schneider a great company and that our commitment to Innovation, Diversity and Sustainability ensures that Life Is On everywhere, for everyone and at every moment.

www.schneider-electric.com

Revision Control:

Version 1 *4 January 2018*	Original Release
Version 1.1 *9 January 2018*	Page 1 - Added link to Product Information - Added recommended recommendations
Version 1.2 *11 January 2018*	Page 2-3 - Added industry cybersecurity best practices
Version 2.0 *22 January 2018*	Page 5-8 - Appendix A added with additional guidance
Version 2.1 *5 February 2018*	Page 7 - Removed remarks for Embedded Systems section

Appendix A. This appendix provides general guidance and background information that might be helpful when planning a mitigation strategy. All information is derived from general industry information. Every case is different and the lines separating the presented product categories may vary in any given situation. Use the information as a guide and not as a standalone plan. User accepts responsibility for proper interpretation of the information for their situation.

Product Category	General Information	Mitigation Strategy	Remarks
Cloud Services	This class reflects offers hosted in the major Cloud platforms; either Microsoft Azure or Amazon AWS. As of the date of writing, the mentioned Cloud platforms have indicated they are patched, and so present no attack surface for these vulnerabilities.	Install operating system patches on IaaS VMs. AWS guidance can be found here - https://aws.amazon.com/security/security-bulletins/AWS-2018-013/. Azure guidance can be found here - https://azure.microsoft.com/en-us/blog/securing-azure-customers-from-cpu-vulnerability/.	Cloud PaaS and SaaS services do not require customer action; both AWS and Azure have patched these services proactively. Microsoft Azure has installed operating system patches and rebooted impacted IaaS VMs.
Mobile/Tablet Services	This class reflects applications that run on smart phones, mobile devices and tablets. These platforms are all known to use vulnerable processors and operating systems. They are directly connected to the Internet. They contain information that is generally accepted as valuable to attackers.	Apply principle of least privilege[1] Restrict multi-user access. Application whitelisting	

[1] every module (such as a process, a user, or a program, depending on the subject) must be able to access only the information and resources that are necessary for its legitimate purpose.

Internet Accessible Application	This class reflects applications that run on either Windows or Linux platforms which are intended to be connected to the Internet. This covers a wide range of applications and services, some may be engineering workstations, design services and supervisory services. They run on top of operating systems that provide attack points to the user. Their connection to the Internet adds this significant attack vector. These devices may contain information of value to attackers as well as provide a “pivot point”; allowing an attack vector to the customer’s infrastructure.	Apply principle of least privilege Restrict multi-user access. Application whitelisting Host and network intrusion prevention system (prevent and monitor), Data loss prevention system	
Restricted Access Applications	This class reflects applications that run on either Windows or Linux platforms. They may provide operational as well as supervisory services. They run on top of operating systems that provide attack points to user . Additionally, they may be directly accessible to a restricted user class, or to all users depending on network architecture. They do not to have connectivity to the Internet, so that removes one substantial attack vector. This fact	Apply principle of least privilege Restrict multi-user access. Application whitelisting Host and network Intrusion prevention system (prevent and monitor), Data loss prevention system	From what is currently known, the most likely exploitation of Spectre would be web-based attacks using JavaScript (for instance in a malicious ad) to leak information, session keys, etc. cached in a browser. Restricted Access Applications have protections against these attack vectors.

	should be verified in the risk assessment. If not properly isolated, it may allow an attack vector to the customer's infrastructure.		
Embedded Systems	This class reflects "purpose built" devices that primarily communicate with other Embedded Systems or Restricted Access Applications. They typically minimize or eliminate human user access to internal command prompts, greatly reducing potential injection points for malware. This class of product generally runs on segregated, isolated network segments; ones that are typically not accessible to users. This class is not meant to be exposed to untrusted networks, as devices are typically not equipped with security capabilities at the device level, and rely heavily on additional layers of defense. Always follow product specific recommendations for configuration and networking.	To attempt an exploit of these vulnerabilities, a threat actor requires network access to a system or device, and the ability to execute untrusted code, particularly, WEB based protocols. Therefore, Schneider Electric's advice continues to be to implement a defense-in-depth strategy with multiple layers of protection such as: **General Security Practices** - Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet. - Ensure physical security of all control system devices and/or systems. - Perform a hazard and risk analysis that considers all hazards resulting from access to (and operation on) PLC devices, and develop cybersecurity and disaster recovery (business continuity) plans accordingly. - Verify that the hardware and software infrastructure that the PLCs are integrated into (along with all organizational measures and rules covering access to the infrastructure) consider the results of the hazard and risk analysis, and are implemented according to practices and standards such as ISA/IEC 62443. - Verify the effectiveness of the IT security and cybersecurity systems using appropriate, proven methods - If certain available features, ports, and services are not needed (particularly WEB), turn them off to reduce potential attack surface. **Additional Mitigations (Local Area Network)** -Place control system networks and devices behind firewalls (such as the ConneXium Tofino Firewalls), and isolate them from the business network - Limit traffic on the local network with managed switches (such as ConneXium managed switches) - Where possible, avoid Wi-Fi capabilities - When Wi-Fi is essential, use only secure communications (such as the latest WPA2 encryption)	

		- Do not grant access to unknown computers **Additional Mitigations (Wide Area Network)** - When remote access is essential, use secure methods such as Virtual Private Networks (VPNs), and ensure the remote access solution(s), as well as the remote computer(s) are kept up-to-date with the latest security patches.	

IoT Devices	This product class reflects special purpose devices like Embedded Systems, but which are designed to send telemetry information to and receive operational instructions from the cloud. Devices purposely built for IoT operation will most likely use affected processors but may or may not use the memory management capabilities of its processor. All interactions with IoT devices are brokered by the cloud, and all connections between the IoT device and the cloud are initiated outbound from the device. Thus, IoT devices should not contain servers (for example, web/ftp/telnet/ssh servers) that accept unsolicited network connections and should not allow human users to access internal command prompts. However, IoT devices that do contain servers or do allow access to internal command prompts are at higher risk of compromise. Risk assessment needs to be made on a device by device basis.	**Mitigations for IoT devices:** - Physical access controls - Network segmentation **Additional mitigations for IoT devices that contain servers or allow access to internal command prompts:** - Disable debug and USB ports - Restrict network access - Account and password security - Apply principle of least privilege - Application whitelisting - Host and Network Intrusion prevention System (prevent and monitor) **Mitigations for cloud applications** - Identity and Access Management governance - Multi-factor authentication for privileged accounts - Access control - Review audit trails	