Security Notification – Spectre and Meltdown

Product Information V3

10-Jan-2018 (Updated on 01-Mar-2018)

Overview

Schneider Electric is actively investigating the impact of Spectre and Meltdown attacks on our offerings. Information will be posted here once it becomes available.

Please Note: Schneider Electric is actively monitoring vendor research into these vulnerabilities. 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.

Please refer to this link for more Information on Spectre and Meltdown: https://www.schneider-electric.com/en/download/document/SEVD-2018-005-01/

Product Information

Based on what is currently known about Spectre and Meltdown:

Low Voltage & Secure Power

- Schneider Electric embedded products and appliances have built in protections intended to limit third party code being executed, designed to mitigate the risk associated with these attacks.
    - These products include but are not necessarily limited to:
        - NetBotz Appliances
        - Network Management Cards
        - Smart-UPS UPSs
        - 3-Phase UPS (Symmetra, Symmetra MW, Gutor, Galaxy, EPS)
        - IT Power Distribution (Rack PDU, Modular, Cabinet, Busway)
        - IT Cooling (InRow, Uniflair, Aquaflair)

        - StruxureWare Data Center Expert Server
        - StruxureWare Data Center Operation
        - Continuum
        - Vista
        - I/Net
        - Com'X
        - PowerLogic Meters
        - Masterpact Breakers
        - EcoStruxure AS line of devices
- For software products running on Windows/Linux/MacOS computers/servers, we advise that system administrators patch the operating systems as recommended by the operating system vendor. Further, Schneider Electric recommends conducting an impact assessment of the performance ramifications of the upgrade prior to applying any upgrade patches.
    - These products include but are not necessarily limited to:
        - PowerChute Business Edition
        - PowerChute Personal Edition
        - PowerChute Network Shutdown
        - StruxureOn Gateway
        - EcoStruxure suite of software products
- For appliance based products packaged with a Linux operating system accessible to users, we advise system administrators to upgrade the operating system as recommended by the operating system vendor. Further, Schneider Electric recommends conducting an impact assessment of the performance ramifications of the upgrade prior to applying any upgrade patches.
    - These products include but are not necessarily limited to:
        - PowerChute Network Shutdown for Virtualization

Medium Voltage

- Schneider Electric embedded products and appliances have built in protections intended to limit third party code being executed, designed to mitigate the risk associated with these attacks.
    - These products include but are not necessarily limited to:
        - Easergy T300 (HU250)
        - EcoStruxure Cyber Security Administrator Expert (SAM)
        - EcoStruxure Substation Operation Gateways (PACIS Gateway)
        - Easergy MICOM PX30

- For software products running on Windows computers/servers, we recommend that system administrators apply operating system patches to Quality Assurance (QA) ENVIRONMENTS and implement basic performance testing. Conducting an impact assessment of the performance ramifications of the upgrade prior to applying upgrade patches is recommended.

    - These products include but are not necessarily limited to:
        - SmartGrid Solution (Electric SCADA, ADMS software and Titanium)
        - Ecostructure Substation Operator Interface (ECOSUI)
        - SFT, Easergy Studio and Easergy PRO Software
        - EcoStructure Cyber Security Administrator tool (SAT)
        - Xflow, L500, Kerwin

Please advise your Schneider Electric support team if require assistance and further analysis: https://www.schneider-electric.com/en/work/support/

To see more information on mitigations please see Appendix A on page 5 here: https://www.schneider-electric.com/en/download/document/SEVD-2018-005-01/

For Schneider Electric SCADA, ADMS software, the table below shows the Schneider Electric test laboratory system configuration along with the tested ADMS/AGMS/ESCADA versions and the applicable patches. Please, note that some Microsoft Windows installation images (builds) may have a KB package with different ID number available for download, but still contain the same patch.

Please, contact your software or hardware vendor's support for any further information about available patches and other recommended mitigation measures.

	ADMS/AGMS Version	ESCADA Version	Vendor	Version	Patch
Hardware	All	All	HP	Gen 9 Blades	*No official patch yet*
Host OS / Hypervisor	All	All	Microsoft	Windows Server 2012 R2 Hyper-V Manager 6.3	KB4056898
VM OS	ADMS 3.2, 3.3, 3.4, 3.5	1.2, 1.3, 1.4, 1.5	Microsoft	Windows Server 2008 R2 SP1	KB4056897
				Windows 7 Enterprise SP1	KB4056897
	ADMS 3.6	1.6	Microsoft	Windows Server 2012 R2	KB4056898
				Windows 7 SP1	KB4056897
	ADMS 3.7, 3.8; AGMS 1.0.9	1.7	Microsoft	Windows Server 2016	KB4056892
				Windows 10 Enterprise	KB4056892

Browser	All		Microsoft	Internet Explorer 11	KB4056568
	All		Google	Chrome	*No official patch yet*

The tests were designed to show performance impacts of the aforementioned patches on the ADMS/AGMS/ESCADA system. Unpatched system baselines were recorded while running performance tests (e.g. services startup/shutdown, database insertions etc.). Then patches were applied and the same performance tests were executed once again. Finally, new measurements were then compared against the baseline. These steps were repeated with different ADMS/AGMS/ESCADA version.

If you have questions or concerns, please contact your Schneider Electric Support team for assistance with test execution: https://www.schneider-electric.com/en/work/support/

If there are no issues after local tests (in test/QA environments) and you decide to proceed to apply the patches to the larger ADMS/AGMS/ESCADA environment, ensure there is a rollback plan ready before you apply patches to production environment.

If the patch testing fails or there are any negative impacts, you may want to try the workarounds suggested by your hardware and software vendors.

Please advise your Schneider Electric support team of test/QA environment test findings that you may believe require assistance and further analysis.

Product Impact

PowerLogic EGX

- According to the latest information from ARM, the CPU used by the EGX, ARM7TDMI, is not susceptible to the Spectre and Meltdown exploit. Schneider Electric will continue to monitor this situation and update as needed.

Patches Available

- **StruxureWare Data Center Operation v8.2.2**
  - Please visit https://help.se-dmaas.com/display/public/UADCO8x/What+is+new+in+StruxureWare+Data+Cen

ter+Operation+8.x to read more and verify your support contracts to get the download link.

- **StruxureWare Data Center Expert v7.5.0**
  - Contact your local Technical Support team to verify whether or not you have a valid software support contract entitling you to receive the StruxureWare Data Center Expert v.7.5.0 update file
  - For more information from Dell on the BIOS update for your Data Center Expert server model :
    - http://www.dell.com/support/article/us/en/19/sln308588/microprocessor-side-channel-vulnerabilities-cve-2017-5715-cve-2017-5753-cve-2017-5754-impact-on-dell-emc-products-dell-enterprise-servers-storage-and-networking-?lang=e

    For more information from Red Hat:

    - https://access.redhat.com/security/vulnerabilities/speculativeexecution
  - For more information on Data Center Expert v7.5.0 please refer to the following:
    - Release Notes: https://help.se-dmaas.com/display/public/UADCE725/StruxureWare+Data+Center+Expert+v7.5.0+Release+Notes
    - Home Page for DCE: https://help.se-dmaas.com/display/public/UADCE725/User+assistance+for+StruxureWare+Data+Center+Expert+7.x+Home

For More Information

THIS DOCUMENT IS INTENDED TO HELP PROVIDE AN OVERVIEW OF THE IDENTIFIED SITUATION AND MITIGATION ACTIONS AND IS NOT INTENDED AS A WARRANTY OR GUARANTEE OF ANY KIND, INCLUDING WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THIS NOTIFICATION, INFORMATION CONTAINED HEREIN, OR MATERIALS LINKED TO IT ARE AT YOUR OWN RISK. WE RESERVE THE RIGHT TO UPDATE OR CHANGE THIS INFORMATION AT ANY TIME AND IN OUR SOLE DISCRETION.

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 related to cybersecurity in Schneider Electric's products, please visit the company's cybersecurity web page:

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 10 *January 2018*	Original Release
Version 1.1 *11 January 2018*	Page 1 - Added link to Security Notification- Spectre and Meltdown Page 2 - Moved EcoStruxure AS line of devices to from last section to first section
Version 2 *18 January 2018*	Page 2 & 3 - Added available patches
Version 2.1 *23 January 2018*	Page 2 - Added product impact section and EGX information
Version 2.2 *25 January 2018*	Page 3 - Updated text around Dell BIOS update.
Version 3 *01 March 2018*	Page 2-4 - Added Product Information for Medium Voltage

Product Security Office

Digitally signed by Product Security Office
DN: cn=Product Security Office, o=Schneider Electric, ou=Global Technology, email=cybersecurity@schneider-electric.com, c=US
Date: 2018.03.01 16:25:44 -05'00'