Life Is On Schneider Electric

Schneider Electric Security Notification

Intel Microarchitectural Data Sampling (ZombieLoad) (V1.3)

12 July 2019 (12 November 2019)

Overview

Schneider Electric is actively investigating the impact of the Intel Microarchitectural Data Sampling vulnerabilities in our offers. Offer specific information will be posted here as it becomes available.

Schneider Electric offers with special or specific recommendations applicable to these vulnerabilities are listed below. As a general recommendation from Schneider Electric, we advise customers to refer immediately to the Intel Microarchitectural Data Sampling Advisory for further information and guidance for any affected systems that may or may not serve as a runtime environment for Schneider Electric software and services.

Schneider Electric continues to monitor and track vendor research into this vulnerability.

Please refer to this link for more Information on the Intel MDS vulnerabilities: https://www.schneider-electric.com/en/download/document/SESB-2019-136-01/

Vulnerability Details

CVE ID: **CVE-2019-11091**

CVSS v3.0 Base Score 5.6 | (Medium) | CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N

Microarchitectural Data Sampling Uncacheable Memory (MDSUM): Uncacheable memory on some microprocessors utilizing speculative execution may allow an authenticated user to potentially enable information disclosure via a side channel with local access. A list of impacted products can be found here: https://www.intel.com/content/dam/www/public/us/en/documents/corporate-information/SA00233-microcode-update-guidance_05132019.pdf

CVE ID: **CVE-2018-12126**

CVSS v3.0 Base Score 5.6 | (Medium) | CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N

Microarchitectural Store Buffer Data Sampling (MSBDS): Store buffers on some microprocessors utilizing speculative execution may allow an authenticated user to potentially enable information disclosure via a side channel with local access. A list of impacted products can be found here: https://www.intel.com/content/dam/www/public/us/en/documents/corporate-information/SA00233-microcode-update-guidance_05132019.pdf

Schneider Electric Security Notification

CVE ID: **CVE-2018-12127**

CVSS v3.0 Base Score 5.6 | (Medium) | CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N

Microarchitectural Load Port Data Sampling (MLPDS): Load ports on some microprocessors utilizing speculative execution may allow an authenticated user to potentially enable information disclosure via a side channel with local access. A list of impacted products can be found here: https://www.intel.com/content/dam/www/public/us/en/documents/corporate-information/SA00233-microcode-update-guidance_05132019.pdf

CVE ID: **CVE-2018-12130**

CVSS v3.0 Base Score 5.6 | (Medium) | CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N

Microarchitectural Fill Buffer Data Sampling (MFBDS): Fill buffers on some microprocessors utilizing speculative execution may allow an authenticated user to potentially enable information disclosure via a side channel with local access. A list of impacted products can be found here: https://www.intel.com/content/dam/www/public/us/en/documents/corporate-information/SA00233-microcode-update-guidance_05132019.pdf

Affected Products and Remediation

Affected Products	Remediation
HMIG5U, PFXSP5B40 (Windows Embedded Standard 7 SP1 32bit) ***All versions***	*This product is End of Life* For assistance with mitigation please contact Schneider Electric Customer Support https://www.schneider-electric.com/en/work/support/contacts.jsp Pro-face Customer Support https://www.proface.com/en/contact
HMIG5U2, PFXSP5B41 (Windows Embedded Standard 7 SP1 32bit) ***All versions***	*Fixed versions planned for April 2020* For assistance with mitigation, please contact the appropriate customer support team listed below. Schneider Electric Customer Support https://www.schneider-electric.com/en/work/support/contacts.jsp Pro-face Customer Support: https://www.proface.com/en/contact

All versions - HMIBMP [Core™ i7 - 4650U 1.7GHz] - PS5000 (modular type) [Core™ i7 - 4650U 1.7GHz] - HMIBMU [Celeron® 2980U 1.6GHz] - PS5000 (modular type) [Celeron® 2980U 1.6GHz] - HMIPSP, HMIPEP [Core™ i3 - 4010U 1.7GHz] - PS5000 (slim type) [Core™ i3 - 4010U 1.7GHz] - HMIPSO [Atom™ - E3827 1.75GHz] - PS5000 (slim type) [Atom™ - E3827 1.75GHz] - HMIBMO, HMIBMI, HMIBSC [Atom™ - E3930 1.3GHz] - PS5000 (modular type) [Atom™ - E3930 1.3GHz]	*Fixed versions planned after February 2020* For assistance with mitigation, please contact the appropriate customer support team listed below. Schneider Electric Customer Support https://www.schneider-electric.com/en/work/support/contacts.jsp Pro-face Customer Support https://www.proface.com/en/contact
All versions - HMIBP, HMIPP [Core™ 2 Duo P8400 2.26GHz] - PS4000B,PS4700,PS4800 Core™ 2 Duo P8400 2.26GHz]	*This product is End of Life* For assistance with mitigation, please contact the appropriate customer support team listed below. Schneider Electric Customer Support https://www.schneider-electric.com/en/work/support/contacts.jsp Pro-face Customer Support https://www.proface.com/en/contact
All versions - HMIPP [Core™ i3-3217UE 1.60 GHz] - PS4600 [Core™ i3-3217UE 1.60 GHz] - HMIPU [Celeron™ 827E 1.40 GHz] - PS4600 Series [Celeron™ 827E 1.40 GHz]	*This product will be End of Life as of July 2019* For assistance with mitigation, please contact the appropriate customer support team listed below. Schneider Electric Customer Support https://www.schneider-electric.com/en/work/support/contacts.jsp Pro-face Customer Support https://www.proface.com/en/contact
All versions - HMIG5UL8A - PFXSP5B41S8A	*This product will be End of Life as of December 2019* For assistance with mitigation, please contact the appropriate customer support team listed below.

	Schneider Electric Customer Support https://www.schneider-electric.com/en/work/support/contacts.jsp Pro-face Customer Support https://www.proface.com/en/contact
All versions - HMIG5UL8B - PFXSP5B41S8B	*Fixed versions planned after April 2020* For assistance with mitigation, please contact the appropriate customer support team listed below. Schneider Electric Customer Support https://www.schneider-electric.com/en/work/support/contacts.jsp Pro-face Customer Support https://www.proface.com/en/contact
All versions - HMIRSP [Intel Xeon quad-core 1225 3.1 GHz] - HMIRXOHCA3W01 [Intel iCore G850, dual core 2.5 GHz] - HMIRSOHPA3W01 [Intel iCore G850, dual core 2.5 GHz] - HMIRXOHCA3001 [Intel iCore G540, dual core 2.5 GHz] - HMIRSUH3A3701 [Intel Core i3 2120 3.3 GHz] - HMIRSUS3A3701 [Intel Core i3 2120 3.3 GHz]	*Fixed versions planned after February 2020* For assistance with mitigation, please contact Schneider Electric Customer Support https://www.schneider-electric.com/en/work/support/contacts.jsp
TelevisGo ***All versions prior to July 2019***	Install hotfix available at https://www.eliwell.com/it/search.html?q=TelevisGo
EcoStruxure Substation Operation Gateway (formerly known as PACiS Gateway) *Affected CPUs: ECU-4784 i7, ECU-4784 Celeron PCCN, RackPC i7, RackPC i5, Box J1900 (UNO-3272), Gateway PCCN (UNO-2272)*	Install Intel Microcode update https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/adv190013

HMI box PC references: Magelis HMIG5U2 Open Box PC, Magelis HMIBMU, HMIBMO, HMIBSU, HMIBMP, HMIPSP industrial PC or standard Windows PC **EcoStruxure Augmented Operator Advisor (AOA)** - AOARS1CZSSPMZZ - AOARS2CZSSPMZZ - AOARS3CZSSPMZZ - AOARM1CZMSPMZZ - AOARM2CZMSPMZZ - AOARM3CZMSPMZZ - AOARX3CZXSPMZZ	These vulnerabilities impact devices on which AOA is running, not AOA directly. Customers using AOA should update their HMI, or the Standard Windows PC they may be using. For assistance with mitigation, please contact Customer Support https://www.schneider-electric.com/en/work/support/contacts.jsp
All versions prior to March 2019 - Ecostruxure Foxboro DCS - Ecostruxure Foxboro SCADA	*Fixed in all versions running: Windows 10 Version 1607 for x64-based Systems, Windows 7 for x64-based Systems Service Pack 1, Windows Server 2008 R2 for x64-based Systems Service Pack 1, Windows Server 2012 R2, Windows Server 2016* Schneider Electric has evaluated the Microsoft Security patches for this vulnerability and made them available to customers through Global Customer support website https://pasupport.schneider-electric.com/home.asp We recommend that customers install the Microsoft May 2019 rollout Security patches following the instructions available at https://pasupport.schneider-electric.com/content/Security/mspatch/mspatch.asp
StruxureWare Data Center Expert (DCE) Hardware Appliances - all models ***Version 7.6 and earlier***	*Fixed in DCE v7.7* Obtain and install upgrade by contacting your local Technical Support https://sxwhelpcenter.ecostruxureit.com/display/public/download/Downloads https://sxwhelpcenter.ecostruxureit.com/display/public/UADCE725/StruxureWare+Data+Center+Expert+v7.7.0+Release+Notes

ADMS ***Versions 3.2 - 3.8***	Versions 3.2, 3.3, and 3.4: Microsoft KB4499164 Monthly rollup https://support.microsoft.com/en-us/help/4499164/windows-7-update-kb4499164 Versions 3.5, 3.6: Microsoft KB4499164 and KB4499151 Monthly rollups https://support.microsoft.com/en-us/help/4499164/windows-7-update-kb4499164 https://support.microsoft.com/en-us/help/4499151/windows-8-1-update-kb4499151 Versions 3.7, 3.8: Microsoft KB4494440 cumulative update: https://support.microsoft.com/en-us/help/4494440/windows-10-update-kb4494440 Additionally, check with your hardware vendor on availability of their software/firmware patches to complete the remediation.
AGMS	Install Microsoft KB4494440 cumulative update: https://support.microsoft.com/en-us/help/4494440/windows-10-update-kb4494440 Additionally, check with your hardware vendor on availability of their software/firmware patches to complete remediation.
Schneider Electric Exchange (https://exchange.se.com) Digital Offers	Host platforms have been patched.
Conext Control - Server ***All versions***	Apply the following Microsoft security patch to the Conext Control server: https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/ADV190013

Conext Advisor 2 - "Conext Gateway" Industrial PC ***All versions***	Apply the following Microsoft security patch to the development server and the production server: https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/ADV190013

General Security Recommendations

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.

For More Information

This document provides an overview of the identified vulnerability or vulnerabilities and actions required to mitigate. For more details and assistance on how to protect your installation, please contact your local Schneider Electric representative and/or Schneider Electric Industrial Cybersecurity Services. These organizations will be fully aware of this situation and can support you through the process.

http://www2.schneider-electric.com/sites/corporate/en/support/cybersecurity/cybersecurity.page

https://www.schneider-electric.com/en/work/services/field-services/industrial-automation/industrial-cybersecurity/industrial-cybersecurity.jsp

Schneider Electric Security Notification

Legal Disclaimer

THIS DOCUMENT IS INTENDED TO HELP PROVIDE AN OVERVIEW OF THE IDENTIFIED SITUATION AND SUGGESTED MITIGATION ACTIONS, REMEDIATION, FIX, AND/OR GENERAL SECURITY RECOMMENDATIONS AND IS PROVIDED ON AN "AS-IS" BASIS WITHOUT WARRANTY OF ANY KIND. SCHNEIDER ELECTRIC DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL SCHNEIDER ELECTRIC BE LIABLE FOR ANY DAMAGES WHATSOEVER INCLUDING DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES, EVEN IF SCHNEIDER ELECTRIC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE USE OF THIS NOTIFICATION, INFORMATION CONTAINED HEREIN, OR MATERIALS LINKED TO IT ARE AT YOUR OWN RISK. SCHNEIDER ELECTRIC RESERVES THE RIGHT TO UPDATE OR CHANGE THIS NOTIFICATION AT ANY TIME AND IN ITS SOLE DISCRETION.

About Schneider Electric

At Schneider, we believe **access to energy and digital** is a basic human right. We empower all to **do more with less**, ensuring **Life Is On** everywhere, for everyone, at every moment.

We provide **energy and automation digital** solutions for **efficiency and sustainability.** We combine world-leading energy technologies, real-time automation, software and services into integrated solutions for Homes, Buildings, Data Centers, Infrastructure and Industries.

We are committed to unleash the infinite possibilities of an **open, global, innovative community** that is passionate with our **Meaningful Purpose, Inclusive and Empowered** values.

www.se.com

Revision Control:

Version 1 *12 July 2019*	**Original Release**
Version 1.1 *17 July 2019*	Remediation section for TelevisGo product updated to remove *Alternatively, disable the Windows' native Remote Desktop feature* (page 4)
Version 1.2 *27 Sep 2019*	Added "Conext Control" and "Conext Advisor 2" products to the Affected Products and Remediation section (pages 6-7)
Version 1.3 *12 Nov 2019*	Updated affected product details for "Conext Control" product (page 6)

Product Security Office

Digitally signed by Product Security Office
Date: 2019.10.24 10:45:10 -04'00'