Schneider Electric Security Notification

Intel Microarchitectural Data Sampling (ZombieLoad) (V6.0)

12 July 2019 (12 October 2021)

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. Schneider Electric advises 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.

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

October 2021 Update: Added remediations for *Conext™ Advisor 2 Cloud, Conext™ Advisor 2 Gateway, Conext™ Control V2 Gateway* (page 2).

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 potentially allow an authenticated user to 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 potentially allow an authenticated user to 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 potentially allow an authenticated user to 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 potentially allow an authenticated user to 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
Conext™ Advisor 2 Cloud **V2.02 and prior**	Microsoft Windows 10 includes a fix for this vulnerability and is available for download here: https://www.microsoft.com/en-in/software-download/windows10 *Reboot is required*
Conext™ Advisor 2 Gateway **V1.28.45 and prior**	Microsoft Windows 10 includes a fix for this vulnerability and is available for download here: https://www.microsoft.com/en-in/software-download/windows10 *Reboot is required*
Conext™ Control V2 Gateway **V2.6 and prior**	Microsoft Windows 10 includes a fix for this vulnerability and is available for download here: https://www.microsoft.com/en-in/software-download/windows10 *Reboot is required*

Schneider Electric Security Notification

HMIG5U SP-5B40 (Atom™ E660T/E680T) **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 (Atom™ E3825) **Versions 05 or prior**	For assistance with mitigation please contact Schneider Electric Customer Support https://www.schneider-electric.com/en/work/support/contacts.jsp
SP-5B41 (Atom™ E3825) **Versions 06 or prior**	For assistance with mitigation please contact Pro-face Customer Support https://www.proface.com/en/contact

HMIPSO
(Atom™ - E3827 1.75GHz)

Reference	Affected Versions	
HMIPSOH552D1801	07 or prior	For assistance with mitigation please contact Schneider Electric Customer Support https://www.schneider-electric.com/en/work/support/contacts.jsp
HMIPSOS552D1801	09 or prior	
HMIPSOC552D1W01	07 or prior	
HMIPSO0552D1001	03 or prior	
HMIPSOH752D1801	06 or prior	
HMIPSOS752D1801	08 or prior	
HMIPSOC752D1W01	06 or prior	
HMIPSO0752D1001	02 or prior	

HMIBMU
(Celeron® 2980U 1.6GHz)

Reference	Affected Versions	
HMIBMUHI29D2801	12 or prior	For assistance with mitigation please contact Schneider Electric Customer Support https://www.schneider-electric.com/en/work/support/contacts.jsp
HMIBMUSI29D2801	13 or prior	
HMIBMUCI29D2W01	12 or prior	

HMIBMU0I29D2001	12 or prior
HMIBMU0I29D200A	12 or prior
HMIBMUHI29D4801	12 or prior
HMIBMUSI29D4801	13 or prior
HMIBMUCI29D4W01	12 or prior
HMIBMU0I29D4001	12 or prior
HMIBMU0I29D400A	12 or prior
HMIBMU0I29DI00A	12 or prior
HMIBMU0I29DE00A	12 or prior

PS5000
(Modular Celeron)

Reference	Affected Versions
PFXPU2*CC*********	10 or prior
PFXPU2*DC*********	10 or prior
PFXPU2*EC*********	10 or prior
PFXPU2*PC*********	10 or prior
PFXPU2*QC*********	10 or prior
PFXPU2*RC*********	10 or prior
PFXPU2*SC*********	10 or prior
PFXPU2*TC*********	10 or prior

For assistance with mitigation please contact Pro-face Customer Support
https://www.proface.com/en/contact

PS5000
(Modular Core i7)

Reference	Affected Versions
PFXPP2*J7*********	12 or prior
PFXPP2*U7*********	13 or prior
PFXPP2*A7*********	12 or prior
PFXPP2*K7*********	12 or prior
PFXPP2*V7*********	12 or prior
PFXPP2*W7*********	13 or prior
PFXPP2*X7*********	12 or prior
PFXPP2*Y7*********	12 or prior
PFXPP2*Z7*********	12 or prior
PFXPP2*L7*********	13 or prior

For assistance with mitigation please contact Pro-face Customer Support
https://www.proface.com/en/contact

PS5000
(Slim model Atom)

Reference	Affected Versions
PFXPS2CNAD4*******	03 or prior
PFXPS2GNAD4*******	02 or prior

For assistance with mitigation please contact Pro-face Customer Support
https://www.proface.com/en/contact

PS5000
(Slim model Core i3)

Reference	Affected Versions
PFXPS2HN3D8*******	05 or prior
PFXPS2KN3D8*******	05 or prior

For assistance with mitigation please contact Pro-face Customer Support
https://www.proface.com/en/contact

PS5000
(Enclosed Core i3)

Reference	Affected Versions
PFXPS2MN3D8******0	02 or prior
PFXPS2MN3D84F0NN0P	04 or prior

For assistance with mitigation please contact Pro-face Customer Support
https://www.proface.com/en/contact

HMIBMP
(Core™ i7 - 4650U 1.7GHz)

Reference	Affected Versions
HMIBMPHI74D2801	12 or prior
HMIBMPSI74D2801	13 or prior
HMIBMP0I74D2001	12 or prior
HMIBMP0I74D200A	12 or prior
HMIBMPHI74D4801	12 or prior
HMIBMPSI74D4801	13 or prior
HMIBMP0I74D4001	12 or prior
HMIBMP0I74D400A	12 or prior
HMIBMP0I74DI00A	12 or prior
HMIBMP0I74DE00A	12 or prior
HMIBMPSI74D470L	13 or prior

For assistance with mitigation please contact Schneider Electric Customer Support
https://www.schneider-electric.com/en/work/support/contacts.jsp

Schneider Electric Security Notification

HMIPSP
(Core™ i3 - 4010U 1.7GHz)

Reference	Affected Versions
HMIPSPH752D1801	08 or prior
HMIPSPS752D1801	09 or prior
HMIPSPC752D1W01	08 or prior
HMIPSP0752D1001	08 or prior
HMIPSPH952D1801	08 or prior
HMIPSPS952D1801	09 or prior
HMIPSPC952D1W01	08 or prior
HMIPSP0952D1001	08 or prior
HMIPSPS752D180L	08 or prior
HMIPSPH752D1701	08 or prior
HMIPSPS752D1701	08 or prior
HMIPSPS752D170L	08 or prior
HMIPSPS952D180L	08 or prior
HMIPSPH952D1701	08 or prior
HMIPSPS952D1701	08 or prior
HMIPSPS952D170L	08 or prior

For assistance with mitigation please contact Schneider Electric Customer Support
https://www.schneider-electric.com/en/work/support/contacts.jsp

HMIPEP
(Core™ i3 - 4010U 1.7GHz)

Reference	Affected Versions
HMIPEPS952D1801	05 or prior
HMIPEP0952D1001	02 or prior

For assistance with mitigation please contact Schneider Electric Customer Support
https://www.schneider-electric.com/en/work/support/contacts.jsp

HMIBMO
(Atom™ - E3930 1.3GHz)

Reference	Affected Versions
HMIBMOMA5DDF10L	03 or prior
HMIBMOMA5DD1E01	02 or prior
HMIBMOMA5DD1101	02 or prior
HMIBMO0A5DD1001	02 or prior
HMIBMO0A5DDF101	03 or prior
HMIBMO0A5DDF10A	03 or prior

For assistance with mitigation please contact Schneider Electric Customer Support
https://www.schneider-electric.com/en/work/support/contacts.jsp

Schneider Electric Security Notification

<table>
<tr><td>

PS5001
(Atom BOX)

Reference	Affected Versions
PFXPL2*1B*4*******	02 or prior
PFXPL2*2B*4*******	03 or prior
PFXPL2*3B*8*******	02 or prior
PFXPL2B3BD80N0NNFC	02 or prior
PFXPL2*4B*8*******	03 or prior

</td><td>

For assistance with mitigation please contact Pro-face Customer Support
https://www.proface.com/en/contact

</td></tr>
<tr><td>

HMIBMI
(Atom™ - E3930 1.3GHz)

Reference	Affected Versions
HMIBMIEA5DD1101	02 or prior
HMIBMIEA5DD110L	02 or prior
HMIBMIEA5DD1E01	02 or prior
HMIBMIEA5DD1001	02 or prior
HMIBMIEA5DD100A	02 or prior

</td><td>

For assistance with mitigation please contact Schneider Electric Customer Support
https://www.schneider-electric.com/en/work/support/contacts.jsp

</td></tr>
</table>

<table>
<tr><td>

HMIBP
HMIPP
PS4000B
PS4700
PS4800
(Core™ 2 Duo P8400 2.26GHz)
All versions

</td><td>

These products are End of Life.

For assistance with mitigation please contact Schneider Electric Customer Support
https://www.schneider-electric.com/en/work/support/contacts.jsp

</td></tr>
<tr><td>

HMIPP (Core™ i3-3217UE 1.60 GHz)
HMIPU (Celeron™ 827E 1.40 GHz)
All versions

</td><td>

These products are End of Life.

For assistance with mitigation please contact Schneider Electric Customer Support
https://www.schneider-electric.com/en/work/support/contacts.jsp

</td></tr>
<tr><td>

PS4600 (Core™ i3-3217UE 1.60 GHz)
PS4600 Series (Celeron™ 827E 1.40 GHz)
All versions

</td><td>

These products are End of Life.

For assistance with mitigation please contact Pro-face Customer Support
https://www.proface.com/en/contact

</td></tr>
</table>

Schneider Electric Security Notification

HMIG5UL8A (Atom™ E660T/E680T) *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
PFXSP5B41S8A (Atom™ E660T/E680T) *All versions*	*This product is End of Life.* For assistance with mitigation please contact Pro-face Customer Support https://www.proface.com/en/contact
HMIG5UL8B (Atom™ E3825) *Versions 01 or prior*	For assistance with mitigation please contact Schneider Electric Customer Support https://www.schneider-electric.com/en/work/support/contacts.jsp

PFXSP5B41S8B (Atom™ E3825) *Versions 01 or prior*	For assistance with mitigation please contact Pro-face Customer Support https://www.proface.com/en/contact
HMIRXOHCA3W01 (Intel iCore G850, dual core 2.5 GHz) HMIRXOHCA3001 (Intel iCore G540, dual core 2.5 GHz) HMIRSOHPA3W01 (Intel iCore G850, dual core 2.5 GHz) HMIRSUH3A3701 (Intel Core i3 2120 3.3 GHz) HMIRSUS3A3701 (Intel Core i3 2120 3.3 GHz) HMIRSP (Intel Xeon quad-core 1225 3.1 GHz) | Reference	Affected Versions | |---|---| | HMIRXOHCA3W01 | 02 or prior | | HMIRXOHCA3001 | 02 or prior | | HMIRSOHPA3W01 | 02 or prior | | HMIRSUH3A3701 | 02 or prior |	For assistance with mitigation please contact Schneider Electric Customer Support https://www.schneider-electric.com/en/work/support/contacts.jsp

Reference	Affected Versions
HMIRXOHCA3W01	02 or prior
HMIRXOHCA3001	02 or prior
HMIRSOHPA3W01	02 or prior
HMIRSUH3A3701	02 or prior

HMIRSUS3A3701	02 or prior
HMIRSPHXA6701	02 or prior
HMIRSPHXA67P1	04 or prior
HMIRSPFXA6701	02 or prior
HMIRSPFXR6702	02 or prior
HMIRSPSXR6S01	04 or prior
HMIRSPSXR6T01	03 or prior

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 the 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

Schneider Electric Security Notification

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 the following industry cybersecurity best practices:

- Locate control and safety system networks and remote devices behind firewalls and isolate them from the business network.
- Install physical controls so no unauthorized personnel can access your industrial control and safety systems, components, peripheral equipment, and networks.
- Place all controllers in locked cabinets and never leave them in the "Program" mode.
- Never connect programming software to any network other than the network for the devices that it is intended for.
- Scan all methods of mobile data exchange with the isolated network such as CDs, USB drives, etc. before use in the terminals or any node connected to these networks.
- Never allow laptops that have connected to any other network besides the intended network to connect to the safety or control networks without proper sanitation.
- Minimize network exposure for all control system devices and 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). Recognize that VPNs may have vulnerabilities and should be updated to the most current version available. Also, understand that VPNs are 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 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.

Revision Control:

Version 1.0 *12 July 2019*	**Original Release**
Version 2.0 *17 July 2019*	Remediation section for TelevisGo product updated to remove *Alternatively, disable the Windows' native Remote Desktop feature* (page 4)
Version 3.0 *27 Sep 2019*	Added "Conext Control" and "Conext Advisor 2" products to the Affected Products and Remediation section (pages 6-7)
Version 4.0 *12 Nov 2019*	Updated affected product details for "Conext Control" product (page 6)
Version 5.0 *14 Jul 2020*	Updated products for HMI (pages 3 to 11)
Version 6.0 *12 Oct 2021*	Added remediations for *Conext™ Advisor 2 Cloud, Conext™ Advisor 2 Gateway, Conext™ Control V2 Gateway* (page 3).