Life Is On Schneider Electric

Schneider Electric Security Bulletin

Wind River VxWorks Vulnerabilities (URGENT/11) V2.13

2 August 2019 (11 May 2021)

Overview

Update: Schneider Electric is aware of a potential exploit available that targets the URGENT/11 vulnerabilities. Our customers should urgently consider applying the remediations or mitigations detailed in this document.

Wind River's VxWorks TCP/IP Stack vulnerabilities have wide-ranging impact across multiple IT and industrial applications. We are working closely with Wind River to understand and assess how these vulnerabilities impact Schneider Electric offers and our customers' operations. We downloaded Wind River's patches as soon as they were made available to us, and we have quickly instituted a remediation plan to evolve all current and future products that rely on the Wind River platform to embed these fixes.

We will continue to monitor and will respond further if new information becomes available. In the meantime, customers should immediately make sure they have implemented cybersecurity best practices across their operations to protect themselves from these vulnerabilities. Where appropriate this includes locating your industrial systems and remotely accessible devices behind firewalls; installing physical controls to prevent unauthorized access; and preventing mission-critical systems and devices from being accessed from outside networks.

Please subscribe to the Schneider Electric security notification service to be informed of updates to this disclosure, including details on affected products and remediations, as well as other important security notifications:

https://www.schneider-electric.com/en/work/support/cybersecurity/security-notifications.jsp

For additional information and support, please contact your Schneider Electric sales or service representative or Schneider Electric's Customer Care Center.

May 2021 Update: Remediation available for Modicon M241 and Modicon M251 Micro PLCs *(page 4)*

Details

Additional details on these specific vulnerabilities can be found on the Wind River security notification webpage:

https://www.windriver.com/security/announcements/tcp-ip-network-stack-ipnet-urgent11/

Of the 11 identified Wind River vulnerabilities, six have the potential to trigger remote code execution. Four of those six can be mitigated by a specific firewall configuration, even if access to the device is required. The other vulnerabilities can trigger denial of service conditions or information disclosure. Important to note, not all vulnerabilities apply to all impacted versions.

Affected Products, Remediations, and Mitigations

Remediating these vulnerabilities requires Schneider Electric to update affected products' firmware. Customers cannot directly apply Wind River patches.

We have downloaded Wind River's patches and have established remediation plans to ensure all current and future Schneider Electric products that rely on the Wind River platform evolve with these embedded fixes. Integrating and validating Wind River's patches requires thorough testing and possibly recertification to ensure the quality of the updated product.

This bulletin will be updated as remediations become available. For all other affected products, customers should refer to mitigations to reduce risk to their installations.

Available Remediations

Industrial Automation Products	Affected Version	Remediation
ConneXium Industrial Firewall/ Router - TCSEFEC2CF3F21 (MM/TX) - TCSEFEC23FCF21 (TX/MM) TCSEFEC23F3F21 (TX/TX)	V5.33 and prior	Software Version 5.37 available here: https://www.schneider-electric.com/en/download/document/TCSEFEC23FxF21/
ConneXium Industrial Firewall - TCSEFEC2CF3F20 (MM/TX) - TCSEFEC23FCF20 (TX/MM) - TCSEFEC23F3F20 (TX/TX)	V5.24 and prior	These models have reached their end of life on January 2015 and are no longer commercially available. Please apply the mitigations proposed and/or upgrade to current models. Contact your local technical support for more information.

E+PLC100 Combination PLC	1.2.0.4 firmware version and prior	Contact your local Eurotherm technical support to get firmware V1.3.0.0.
E+PLC400 Combination PLC	1.2.0.4 firmware version and prior	Contact your local Eurotherm technical support to get firmware V1.3.0.0.
HMIGXU	V1.1.0.32 and prior	Contact your local technical support to get the Vijeo Basic runtime V1.1.0.4404 software
Magelis HMI - HMIGTO Series, HMISCU Series, HMIGTUX Series, and HMIGTU Series (Except Open BOX)	Vijeo Designer V6.2 SP9 and prior	Contact your local technical support to get the Vijeo Designer V6.2 SP9 HotFix1 Alpha4.
Modicon X80 I/O modules: - Modicon X80 BMEAHI0812 HART Analog Input Module - Modicon X80 BMEAHO0412 HART Analog Output Module - Modicon Network Option Switch BMENOS0300 (C) - I/O Drop Adapters – BMXCRA31200, BMXCRA31210 (C), BMECRA31210 (C)	- BMEAHI0812 and BMEAHO0412: V1.30 and prior - BMENOS0300 (C): V1.01 and prior - BMXCRA31200, BMXCRA31210 (C), and BMECRA31210 (C): V2.40 and prior	BMEAHI0812: https://www.se.com/ww/en/download/document/BMEAHI0812_Firmware_upgrade/ BMEAHO0412: https://www.se.com/ww/en/download/document/BMEAHO0412_Firmware_upgrade/ BMENOS0300 (C): https://www.se.com/ww/en/download/document/BMENOS0300_Firmware_/ BMXCRA31200: https://www.se.com/ww/en/download/document/BMXCRA31200_FW_and_FW_History BMXCRA31210 (C): https://www.se.com/ww/en/download/document/BMXCRA31210_FW_and_FW_History BMECRA31210 (C): https://www.se.com/ww/en/download/document/BMECRA31210_FW_and_FW_History

Modicon LMC078 Controller	V1.51.15.05 and prior	Firmware update is available through Schneider Electric Software Update (SESU). Download the SESU client here https://www.seupdate.schneider-electric.com/download/SystemConsistency/SoftwareUpdate/SESU_231/SESU_2.3.1_setup_sfx.exe
Modicon M241 Micro PLC	Firmware versions prior to V5.1.9.14	Firmware is available through SESU update or in Machine Expert 2.0 available in the following link: https://www.se.com/ww/en/product-range-download/2226-ecostruxure-machine-expert/#/software-firmware-tab
Modicon M251 Micro PLC	Firmware versions prior to V5.1.9.14	Firmware is available through SESU update or in Machine Expert 2.0 available in the following link: https://www.se.com/ww/en/product-range-download/2226-ecostruxure-machine-expert/ - /software-firmware-tab
Modicon M262 Logic/Motion Controller	Firmware V5.0.3.2 and prior	Firmware update is the Schneider Electric Software Update (SESU). Download the SESU client here https://www.update.schneider-electric.com/download/SystemConsistency/SoftwareUpdate/SESU_220/SESU_2.2.0_setup_sfx.exe
Modicon M580 Ethernet Communications Modules	Modicon M580 Ethernet Communications Modules: BMENOC0301 BMENOC0311 BMENOC0321	BMENOC0301: https://www.se.com/ww/en/download/document/BMENOC0311+Exec+and+Release+Notes/ BMENOC0311: https://www.se.com/ww/en/download/document/BMENOC0301+Exec+and+Release+Notes/ BMENOC0321: https://www.se.com/ww/en/download/document/BMENOC0321_Firmware/

Modicon M580 Ethernet communications Modules Modicon M580 IEC 61850 - BMENOP0300 (C)	V2.1 and prior	A fix is available in version 2.2: https://www.se.com/ww/en/product/BMENOP0300/m580-iec-61850-communication-module/
Modicon M580 ePAC CPUs including Safety CPUs	M580 V2.90 and prior	A fix is available on Modicon M580 firmware V3.10, find links to fixed versions in the Download Links section
Modicon MC80 Programmable Logic Controller	V1.4 and prior	A fix is available in version 1.5: https://www.se.com/ww/en/product-range-download/62396-modicon-mc80/?filter=business-1-industrial-automation-and-control#/software-firmware-tab
Modicon Momentum Unity	V2.01 and prior	A fix is available in SV2.10 - https://www.se.com/ww/en/download/document/Momentum_FW_update/
Modicon Quantum Ethernet DIO network module - 140NOC78x00 (C)	All versions	These models have reached their end of life. Please apply the mitigations proposed and/or upgrade to Modicon M580 offer. Contact your local technical support for more information.
Modicon Quantum 140 CRA	V2.40 and prior	A fix is available in V2.50, available here: 140CRA31200: https://www.se.com/ww/en/download/document/_140CRA31200_FW_and_FW_History 140CRA31908: https://www.se.com/ww/en/download/document/_140CRA31908_FW_and_FW_History
Modicon Quantum Head 140 CRP module - 140CRP31200 (C)	All versions	These models have reached their end of life. Please apply the mitigations proposed and/or upgrade to Modicon M580 offer. Contact your local technical support for more information.

Modicon Quantum 140 NOP Communications Module	All versions	These models have reached their end of life in December 2018 and are no longer commercially available. Please apply the mitigations proposed and/or upgrade to IEC 61850 communication module BMENOP0300. Contact your local technical support for more information.
Nanodac Recorder / Controller	V8.14 and prior	A fix is available in V8.16 - https://www.eurotherm.com/?wpdmdl=28419
PacDrive 3 Eco/Pro/Pro2 Motion Controllers	V1.62.5.6 and prior	Firmware is available in Machine Expert 1.2 available in the following link: https://www.se.com/ww/en/product-range-download/2226-ecostruxure-machine-expert/#/software-firmware-tab
Pro-face HMI -GP4000H/R/E Series, GP4100 Compact Series, LT4000M Modular Series, GP4000E Series, IoT Gateway, SP5000 Series, and SP5000X Series	GP-ProEX V4.09.100 and prior (HMI version is dependent on using GP-Pro EX version)	Firmware update is available through GP-Pro EX software. GP-Pro EX is available in the following link: https://www.proface.com/en/download/update/gpproex/v409
SCADAPack 53xE RTUs	V8.14.7 and prior	Contact your local technical support or email supportTRSS@se.com for the latest version.
SCADAPack 57x RTUs	V9.2.3 and earlier	Contact your local technical support or email supportTRSS@se.com for the latest version.
SCD6000 Industrial RTU	V7.0.34 SY-1101207_G17 and prior	A fix is available in V7.0.36 SY-1101207_G18. Contact your local technical support for more information.
Tricon Communication Modules	TCM/TCM2 V11.1 - V11.4	https://pasupport.schneider-electric.com/

Trident Communication Integration Module	V3.0	https://pasupport.schneider-electric.com/
versadac™ Scalable Data Recorder	V2.37 firmware version and prior	Contact your local Eurotherm technical support to obtain firmware V2.41.
Energy Management Products	**Affected Version**	**Remediation**
Easergy MiCOM C264	Versions prior to D5.24 – C264 D5.X [For PACiS (ESO) 6.3] Versions prior to 1.79 – C264 D1.X [For PACiS (ESO) 5.2] Versions prior to D4.25 – C264 D4.X [For PACiS (ESO) 6.1]	Contact your local technical support or the Energy Application Center (EAC) for assistance in upgrading to the new version.
Easergy MiCOM P30	P30 with rejuvenated Ethernet board CORTEC with v66x; v670	Contact your local technical support or the Energy Application Center (EAC) for assistance in upgrading to the new version
Easergy MiCOM Px40	All P40 with rejuvenated Ethernet board CORTEC with digit 7= Q, R or S	Contact your local technical support or the Energy Application Center (EAC) for assistance in upgrading to the new version
Easergy P5	Firmware version: V01 Release: 001.029 Date: 29th May 2019	Firmware version: V01 Release: 200.008 Release date: 15th Nov 2019 Please Contact your local technical support for assistance.

Easergy T300 (SC150 & LV150)	Firmware 1.5.2 and earlier	Contact your local technical support or the Energy Application Center (EAC) for assistance in upgrading to the new version – 2.7.
ION7400	V2.1.0 and earlier	https://www.se.com/us/en/download/document/ION7400_meter_FW_v002.002.001/
ION7400 MID (METSEION74001)	V002.100.000 firmware version and earlier	V002.002.001 https://www.se.com/ca/en/download/document/ION7400_MID_meter_FW_v2.2.1/
ION9000	V2.1.0 and earlier	https://www.se.com/us/en/download/document/ION9000_meter_FW_v002.002.001/
PM8000	V2.1.0 and earlier	https://www.se.com/us/en/download/document/PM8000_meter_FW_v002.002.001/
PM8000 MID (METSEPM82401)	V002.100.000 firmware version and earlier	V002.002.001 https://www.se.com/ca/en/download/document/PM8000_MID_meter_FW_v2.2.1/
SAGE RTU	K3 firmware and earlier for C3414 CPU	https://www.sage-rtu.com/updates/c3414-500-s02k4-firmware-release
Saitel DR with HU_A CPU	Version: 11.04.17 and earlier.	Contact your local technical support or the Energy Application Center (EAC) for assistance in upgrading to the new version.
TeSys island	Version TeSysisland_001.100.013.sedp (01.0100)	Download version TeSysisland_002.100.013.sedp (02.0100) or later version. Download link: https://www.se.com/us/en/download/document/TeSysisland_002.100.013.zip/ (also available via SoMove with the installed DTM)

Mitigations

Since the vulnerabilities are present in the TCP/IP stack of the VxWorks product, an active network connection is required to exploit them. Therefore, Schneider Electric customers can act now to mitigate the risk of attack by limiting access to their devices, which would immediately reduce attempted exploits:

- Limit access to the networks on which Schneider Electric devices are placed.
- Do not expose Schneider Electric devices directly to the internet.
- Restrict external network connectivity to the affected devices.
- Always place Schneider Electric devices behind firewalls and/or other security protection appliances that limit access only to authorized remote connections.
- Continually monitor affected devices for security events that could warn of attempted unauthorized access.
- Limit access to internal networks where devices reside.

For more details and assistance on how to protect your installation, please contact your local Schneider Electric's Industrial Cybersecurity Services organization, which is fully aware of this situation and can support you through the process.

Download Links

M580 V3.10 Firmware	
BMEP584040	https://www.schneider-electric.com/en/download/document/M580_BMEP584040_SV3.10/
BMEH584040 and C	https://www.schneider-electric.com/en/download/document/M580_BMEH584040_SV3.10/
BMEP586040 and C	https://www.schneider-electric.com/en/download/document/M580_BMEP586040_SV3.10/
BMEH586040 and C	https://www.schneider-electric.com/en/download/document/M580_BMEH586040_SV3.10/
BMEP581020 and H	https://www.schneider-electric.com/en/download/document/M580_BMEP581020_SV3.10/
BMEP582020 and H	https://www.schneider-electric.com/en/download/document/M580_BMEP582020_SV3.10/
BMEP582040 and H	https://www.schneider-electric.com/en/download/document/M580_BMEP582040_SV3.10/

BMEP583020	https://www.schneider-electric.com/en/download/document/M580_BMEP583020_SV3.10/
BMEP583040	https://www.schneider-electric.com/en/download/document/M580_BMEP583040_SV3.10/
BMEP584020	https://www.schneider-electric.com/en/download/document/M580_BMEP584020_SV3.10/
BMEP585040 and C	https://www.schneider-electric.com/en/download/document/M580_BMEP585040_SV3.10/
BMEH582040 and C	https://www.schneider-electric.com/en/download/document/M580_BMEH582040_SV3.10/
BMEP584040S	https://www.schneider-electric.com/en/download/document/M580_BMEP584040S_SV3.10/
BMEH584040S	https://www.schneider-electric.com/en/download/document/M580_BMEH584040S_SV3.10/
BMEH586040S	https://www.schneider-electric.com/en/download/document/M580_BMEH586040S_SV3.10/
BMEP582040S	https://www.schneider-electric.com/en/download/document/M580_BMEP582040S_SV3.10/

Additional Security Recommendations

We also strongly recommend applying the following industry cybersecurity best practices:

- 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 recently disclosed Wind River VxWorks vulnerabilities and actions required to mitigate them.

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

Legal Disclaimer

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:

Schneider Electric Security Bulletin

Version 1 *2-Aug-2019*	Original Release
Version 1.1 *7-Aug-2019*	Added *Modicon LMC078* Controller to list of affected products, and removed a duplicate product (page 3)
Version 1.2 *9-Aug-2019*	Added *SAGE RTU* to list of affected products (page 4)
Version 1.3 *19-Aug-2019*	Removed *Modicon M580 Ethernet / Serial RTU Module* and added *Modicon eX80 - BMEAHI0812 HART Analog Input Module* to list of affected products (page 3)
Version 1.4 *29-Aug-2019*	Updated affected versions for Easergy MiCOM C264 product (page 3)
Version 2.0 *11-Oct-2019*	- Exploit information added to Overview Section (page 1) - Remediations added for *SAGE RTU*, *Easergy* MiCOM *C264, and SCADAPack 57x RTUs* (page 2) - Updated affected versions for *Easergy* MiCOM *P40* (page 3)
Version 2.1 *17-Oct-2019*	Updated affected versions for *SCADAPack 57x RTUs* and *SAGE RTU* under Available Remediations (page 2)
Version 2.2 *12-Nov-2019*	Updated Remediations for *ConneXium Industrial Firewall*, *Easergy* MiCOM *C264 Controller* (page 2-3) Enhanced product list with additional details for *Modicon X80 I/O modules.* Added *Modicon Quantum Head 140 CRP*, *Modicon Momentum Unity*, and removed *TMSES4 Ethernet Module* from affected products (page 3-4)
Version 2.3 *13-Nov-2019*	Updated Remediations for *Modicon M262 Logic/Motion Controller* (page 3)
Version 2.4 *10-Dec-2019*	Updated Remediations for *Modicon M580 Ethernet Communications Modules, Modicon M580 ePAC CPUs including Safety CPUs, Easergy P5, ION7400, ION9000, PM8000* (page 3-4)
Version 2.5 *14-Jan-2020*	Updated Remediations for *Modicon X80 I/O modules, Modicon Momentum Unity, Nanodac Recorder / Controller (added to affected products), SCADAPack 53xE RTUs, and Saitel DR with HU_A CPU* (page 3-5)
Version 2.6 *11-Feb-2020*	Updated Remediations for *Modicon LMC078 Controller, Modicon M580 Ethernet communications Modules : Modicon M580 IEC 61850 - BMENOP0300 (C), Modicon MC80 Programmable Logic Controller, Modicon Quantum 140 NOP Communications Module, PacDrive 3 Eco/Pro/Pro2 Motion Controllers, Pro-face HMI -GP4000H/R/E Series, GP4100 Compact Series, LT4000M Modular Series,*

	GP4000E Series, IoT Gateway, SP5000 Series, and SP5000X Series, Easergy MiCOM *Px40, and TeSys island* (page 3-6)
Version 2.7 *11-Mar-2020*	Updated Remediations for *HMIGXU, Easergy MiCOM P30, Tricon Communication Modules, Trident Communication Integration Module* (page 3 and 5)
Version 2.8 *14-Apr-2020*	Updated Remediations for *ION7400 MID and PM8000 MID* (page 6)
Version 2.9 *12-May-2020*	Updated Remediations for *Modicon Network Option Switch, Modicon X80 - I/O Drop Adapters, Modicon Quantum 140 CRA, Modicon Quantum Head 140 CRP, and Modicon Quantum Ethernet DIO network module - 140NOC78x00 (C), SCD6000 Industrial RTU, Pro-face HMI -GP4000H/R/E Series* (page 3, 5, and 6)
Version 2.10 *21-May-2020*	Clarified "Affected Version" and "Remediation" version reference numbers for *SCD6000 Industrial RTU* product (page 6).
Version 2.11 *9-Jun-2020*	Updated Remediations for *Easergy T300* and *Magelis HMI - HMIGTO Series, HMISCU Series, HMIGTUX Series, and HMIGTU Series (Except Open BOX)* products. (pages 3 and 7)
Version 2.12 *13-Oct-2020*	Updated Remediations for *versadac™ Scalable Data Recorder, E+PLC100 Combination PLC*, and *E+PLC400 Combination PLC* products. (pages 3 and 6)
Version 2.13 11-May-2021	Updated Remediations for Modicon M241 Micro PLC and Modicon M251 Micro PLC (page 4)

Product Security Office

Digitally signed by Product Security Office
Date: 2021.05.08 21:37:15 -04'00'