Life Is On Schneider Electric

Schneider Electric Security Notification

Treck TCP/IP Vulnerabilities (Ripple20) (V2.14)

23 June 2020 (10 Aug 2021)

Overview

Schneider Electric is aware of multiple vulnerabilities affecting Treck Inc.'s embedded TCP/IP stack, collectively known as Ripple20, which Treck disclosed publicly on June 16. The vulnerabilities range in severity and therefore have varying levels of risk.

Schneider Electric continues to assess how the newly disclosed vulnerabilities affect its offers. The company will continue to update this notification as additional offer-specific information becomes available.

Customers should immediately ensure they have implemented cybersecurity best practices across their operations to protect themselves from possible exploitation of these vulnerabilities. Where appropriate, this includes locating their industrial systems and remotely accessible devices behind firewalls; installing physical controls to prevent unauthorized access; preventing mission-critical systems and devices from being accessed from outside networks; and following the remediation and general security recommendations below.

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

August 2021 Update: Corrected download links for *TM3 bus coupler modules – EIP/SL/CANOpen* (page 2-3)

Affected Products & Remediations

Schneider Electric has determined that the following offers are impacted. The company will update this table as it continues to assess the impact these vulnerabilities have on its offers.

Please subscribe to the Schneider Electric security notification service to be informed of critical updates to this notification, including information on affected products and remediation plans: https://www.se.com/ww/en/work/support/cybersecurity/security-notifications.jsp

Available Remediations

Industrial Automation Products	Affected Versions	Remediation/Mitigation
ATV340E Altivar Machine Drives	All Versions prior to V3.2IE25	A fix is now available in product releases V3.2IE25 and above. For product release prior to V3.2IE25, apply the mitigations detailed in the Recommended Mitigations section and contact your local technical support for more information.
ATV630/650/660/680/6A0/6B0 Altivar Process Drives	All Versions prior to V3.3IE33	A fix is now available in product releases V3.3IE33 and above. For product release prior to V3.3IE33, apply the mitigations detailed in the Recommended Mitigations section and contact your local technical support for more information.
ATV930/950/960/980/9A0/9B0 Altivar Process Drives	All Versions prior to V3.3IE26	A fix is now available in product releases V3.3IE26 and above. For product release prior V3.3IE26, apply the mitigations detailed in the Recommended Mitigations section and contact your local technical support for more information.
SCADAPack 32 RTU	All versions prior to V2.25	Telepace Studio must be used to update the SCADAPack 32 RTU firmware to version 2.25 or newer. Download and install Telepace Studio 5.4.2 or newer from https://shop.exchange.se.com/en-US/apps/55670
TM3BC bus coupler module – EIP	All versions prior to V2.2.1.1	A fix is now available in firmware version V2.2.1.1 available for download below: https://www.se.com/ww/en/download/document/TM3BC_EIP_2_2_1_1/

TM3BC bus coupler module - SL	All versions prior to V2.1.1.1	A fix is now available in firmware version V2.1.1.1 available for download below: https://www.se.com/ww/en/download/document/TM3BC_MBSL_2_1_1_1/
TM3BC bus coupler module - CANOpen	All versions prior to V2.1.1.1	A fix is now available in firmware version V2.1.1.1 available for download below: https://www.se.com/ww/en/download/document/TM3BC_CO_2_1_1_1/
VW3A3310 Altivar 61/71 Modbus TCP option	All Versions (V2.1IE09 and prior)	This is an End Of Commercialization offer that is replaced by the ALTIVAR 900 & ALTIVAR 600 ranges. To reduce risk of exploitation, apply the mitigations detailed in the Recommended Mitigations section.
VW3A3310D Altivar 61/71 Ethernet daisy chain option	All Versions (V3.0IE11 and prior)	This is an End Of Commercialization offer that is replaced by the ALTIVAR 900 & ALTIVAR 600 ranges. To reduce risk of exploitation, apply the mitigations detailed in the Recommended Mitigations section.
VW3A3316 Altivar 61/71 Ethernet IP option	All Versions (V1.2IE14 and prior)	This is an End Of Commercialization offer that is replaced by the ALTIVAR 900 & ALTIVAR 600 ranges. To reduce risk of exploitation, apply the mitigations detailed in the Recommended Mitigations section.

VW3A3320 Altivar 61/71 Ethernet IP RSTP option	All Versions (V1.1IE19 and prior)	This is an End Of Commercialization offer that is replaced by the ALTIVAR 900 & ALTIVAR 600 ranges. To reduce risk of exploitation, apply the mitigations detailed in the Recommended Mitigations section.
XUPH001 OsSense communication module	All versions	This offer is not affected by CVE-2020-11897, CVE-2020-11899, CVE-2020-11900, CVE-2020-11902, CVE-2020-11903, CVE-2020-11905, CVE-2020-11908, CVE-2020-11913. For other CVEs, the CVSS score is evaluated as Medium in the product context. To reduce risk of exploitation, apply the mitigations detailed in the Recommended Mitigations section.
XGCS850C201 OsiSense RFID compact smart antenna	All versions	This offer is not affected by CVE-2020-11897, CVE-2020-11899, CVE-2020-11900, CVE-2020-11902, CVE-2020-11903, CVE-2020-11905, CVE-2020-11908, CVE-2020-11913. For other CVEs, the CVSS score is evaluated as Medium in the product context. To reduce risk of exploitation, apply the mitigations detailed in the Recommended Mitigations section.
VW3A3720, VW3A3721 Altivar Process Communication Modules	All Versions prior to V1.15IE25	A fix is available in product releases V1.15IE25 and above. For product release prior V1.15IE25, apply the mitigations detailed in the Recommended Mitigations section and contact your local technical support for more information.
ZBRCETH Modbus TCP communication module for ZBRN1 Harmony Hub	SV:02.04, PV:02, RL:02 and prior	A fix is now available in product releases SV:02.05, PV:03, RL:03 and above. For product release prior to SV:02.05, PV:03, RL:03, apply the mitigations detailed in the Recommended Mitigations section and contact your local technical support for more information on upgrading to SV:02.05.

Schneider Electric Security Notification

Energy Management Products	Affected Versions	Remediation/Mitigation
ACE850 Sepam communication interface	All versions	The ACE850 ethernet module for SEPAM protection relays is a product designed to be operated on a secure network. To minimize the risk from both Ripple 20 and the network-accessible functions of the relay we recommend that concerned customers: - Enable the IP-based filtering capability in the ACE850 - Place strong, active controls on the network hosting the ACE850 - Consider moving to a newer relay such as the Easergy series if product-level access protections are required To reduce risk of exploitation, apply the mitigations detailed in the Recommended Mitigations section.
Acti9 Smartlink EL B A9XELC08	All versions	This is an End of Commercialization Offer. If possible, this product should be replaced by PowerTagLink-C (commercial reference A9XELC10 for which a patch is available from version 1.7.5 or greater. For specific applications not supported by PowerTag Link C (pulse metering, Acti9 RCA, Acti9 iPF+SD 24), apply the mitigation detailed in the Recommended Mitigation section.
Acti9 Smartlink IP	All versions	This is an End of Commercialization offer. If possible, this product should be replaced by Smartlink SIB (commercial reference : A9XMZA08) for which a patch is available in FW version 2.18 or greater. To reduce risk of exploitation, apply the mitigations detailed in the Recommended Mitigations section.

Schneider Electric Security Notification

Acti9 PowerTag Link C	1.7.4 firmware version and earlier	Use the Schneider Electric eSetup for Electrician V6.2 mobile app, available below, to download and apply the latest firmware for Acti9 PowerTag Link C which contains a fix for these vulnerabilities. Google Play Store for Android devices: https://play.google.com/store/apps/details?id=com.schneiderelectric.ConfigElec Apple App Store for Apple devices: https://apps.apple.com/au/app/esetup-for-electrician/id1087855591
Acti9 PowerTag Link / HD	Versions prior to 001.008.007	Customers should update firmware using EcoStruxure Power Commission (EPC) installer V7.0 available here: https://www.se.com/ww/en/product-range-download/64482-acti9-powertag-link/?selected-nodeid=12492093362#/software-firmware-tab
Acti9 Smartlink SI D	Versions prior to 002.004.002	Customers should update firmware using EcoStruxure Power Commission (EPC) installer V7.0 available here: https://www.se.com/ww/en/product-range-download/64482-acti9-powertag-link/?selected-nodeid=12492093362#/software-firmware-tab
Acti9 Smartlink SI B		
EGX150/Link150 Ethernet Gateway	V5.1.15 and prior	A fix is available in V5.1.18: https://www.se.com/ww/en/product-range-download/63423-link150/?selected-node-id=12366756685 - /software-firmware-tab
eIFE Ethernet Interface for MasterPact MTZ drawout circuit breakers	Firmware versions earlier than V4.001.000	The firmware is available through EcoStruxure Power Commission (EPC) software V2.18. The updated version of EPC is available here: https://www.se.com/ww/en/download/document/Ecoreach_Installer/

EcoStruxure Building SmartX IP MP Controllers	All versions	All issues remediated in the 3.02.02 release, and higher. Update files can be found on the Schneider Electric Exchange https://ecoxpert.se.com/ -- 1. Search for 'relebov3.2.1' 2. Set the Filter criteria to RN or Firmware, as required.
EcoStruxure Building SmartX IP RP Controllers	All versions	All issues remediated in the 3.02.02 release, and higher. Update files can be found on the Schneider Electric Exchange https://ecoxpert.se.com/ 1. Search for 'relebov3.2.1' 2. Set the Filter criteria to RN or Firmware, as required.
IFE Ethernet Interface for ComPact, PowerPact, and MasterPact circuit breakers	Firmware versions earlier than V4.001.000	The firmware is available through EcoStruxure Power Commission (EPC) software V2.18. The updated version of EPC is available here: https://www.se.com/ww/en/download/document/Ecoreach_Installer/
IFE Gateway	Firmware versions earlier than V3.011.003	The firmware is available through EcoStruxure Power Commission (EPC) software V2.18. The updated version of EPC is available here: https://www.se.com/ww/en/download/document/Ecoreach_Installer/
PowerLogic EGX100 Ethernet Gateway	Versions 3.0 and newer	This is an End of Commercialization offer. If possible, this product should be replaced by Link 150 (commercial reference: EGX150) for which a patch is available in FW version 5.1.18 or greater. To reduce risk of exploitation, apply the mitigations detailed in the Recommended Mitigations section.
PowerLogic EGX300 Ethernet Gateway	All versions	This is an End of Commercialization offer. If possible, this product should be replaced by Com'X510 (commercial reference: EBX510) which is not impacted by this vulnerability. To reduce risk of exploitation, apply the mitigations detailed in the Recommended Mitigations section.

PowerLogic PM5000 series power meters	Specified in Download Links section	See Download Links section of this document for the complete list of PowerLogic PM5000 series models and the respective remediated versions available for download.
APC Network Management Card 1 (NMC1) - AP9617, AP9618, AP9619 Devices with an embedded Network Management Card 1 include (but are not limited to): Metered/Switched Rack PDUs (AP78XX, AP79XX), Rack Automatic Transfer Switches (AP77XX), Environmental Monitoring Units (AP9320, AP9340, NetBotz 200). **APC Network Management Card 2 (NMC2) - AP9630/30CH/30J, AP9631/31CH/31J, AP9635/35CH, AP9537SUM** Devices with an embedded Network Management Card 2 include (but are not limited to): 2G Metered/Switched Rack PDUs (AP84XX, AP86XX, AP88XX, AP89XX), Rack Automatic Transfer Switches (AP44XX), Certain Audio/Video Network Management Enabled products, Smart-UPS Online (SRT). **APC Network Management Card 3 (NMC3) - AP9640, AP9641**		Refer to Security Notification SEVD-2020-174-01 document for remediation and mitigations on all APC Network Management Card models.

Affected Products

Industrial Automation Products	Affected Version
ATV6000 Medium Voltage Altivar Process Drives	All Versions (V1.1IE02 and earlier)
Energy Management Products	**Affected Version**
Acti9 Smartlink EL D	All versions
TeSys T LTMR08EBD Motor Controller	All versions
Wiser Energy IP module by Schneider Electric (EER31800)	All versions
Wiser Energy IP module by Clipsal (EER72600)	All versions

Gateway Connector by Elko (EKO01827)	All versions
Andover Continuum controller models: - NetController 1 (NC1) = Model CX9900 - NetController 2 (NC2) = Model CX9680 - ACX2 = Model ACX5720 and ACX5740 - CX9200 series - CX9400 series - CX9924 - CX9702 - BCX4040 series - BCX9640 series	All versions

Recommended Mitigations

Since the vulnerabilities are present in the TCP/IP stack, 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.

For devices on a local network:

- Network Partitioning: Locate devices behind firewalls capable of deep packet inspection with rulesets limiting access with only approved protocols and functions and to only those devices and endpoints requiring access.
- Anomalous IP traffic: Block and detect anomalous IP traffic and malformed packets. Refer to the Solution section of the CERT-Coordination Center Vulnerability Note VU#257161 for details.
- Disable DHCP on the NMC and configure it to use a static IP address.
- To avoid the use of DNS, set DNS servers to 0.0.0.0 and utilize static IP addresses for all servers the NMC will connect.
- If DNS must be used, then normalize DNS through a secure recursive server or application layer firewall
- Enable only secure remote access methods. Disable any insecure protocols.

For devices that must communicate via the Internet:

- Minimize network exposure for embedded and critical devices, keeping exposure to the minimum necessary, and ensuring that devices are not accessible from the Internet unless absolutely essential.

If network access is not required:

- Remove the Ethernet cable from the affected device.

Additional mitigations:

- Access Controls: Install physical and logical controls so no unauthorized personnel or device can access your systems, components, peripheral equipment, and networks.

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

Vulnerability Details

- CVE-2020-11896
- CVE-2020-11897
- CVE-2020-11898
- CVE-2020-11899
- CVE-2020-11900
- CVE-2020-11901
- CVE-2020-11902
- CVE-2020-11903
- CVE-2020-11904
- CVE-2020-11905
- CVE-2020-11906
- CVE-2020-11907
- CVE-2020-11908
- CVE-2020-11909
- CVE-2020-11910
- CVE-2020-11911
- CVE-2020-11912
- CVE-2020-11913
- CVE-2020-11914

Additional details on these specific vulnerabilities can be found on the ICS-CERT Advisory at https://www.us-cert.gov/ics/advisories/ICSA-20-168-01.

Download Links

PowerLogic PM5000 Series Power Meters

PowerLogic PM5000 Model	Affected Version	Remediation/Mitigation
PM5560 PM5563 PM5580	V2.7.8 and earlier	A fix in V2.8.3 is now available for download: https://download.schneider-electric.com/files?p_enDocType=Firmware&p_File_Name=PM5560_PM5563_PM5580_V2.8.3_Release.zip&p_Doc_Ref=PM5560_PM5563_PM5580
PM5561	V10.7.1 and earlier	A fix in V10.7.3 is now available for download: https://download.schneider-electric.com/files?p_enDocType=Firmware&p_File_Name=PM5561_upgrade_10.7.3_Release.zip&p_Doc_Ref=PM5561

PM5650	V2.10.1 and earlier	A fix in V2.11.2 is now available for download: https://download.schneider-electric.com/files?p_enDocType=Firmware&p_File_Name=PM5650_upgrade_V2.11.2_Release.zip&p_Doc_Ref=PM5650
PM5570	V3.1.0 and earlier	A fix in V3.1.3 is now available for download: https://download.schneider-electric.com/files?p_enDocType=Firmware&p_File_Name=PM5570_upgrade_V3.1.3_Release.zip&p_Doc_Ref=PM5570
PM5660	V3.1.1 and earlier	A fix in V3.1.3 is now available for download: https://download.schneider-electric.com/files?p_enDocType=Firmware&p_File_Name=PM5660_upgrade_V3.1.3_Release.zip&p_Doc_Ref=PM5660
PM5760	V3.1.1 and earlier	A fix in V3.1.3 is now available for download: https://download.schneider-electric.com/files?p_enDocType=Firmware&p_File_Name=PM5760_upgrade_V3.1.3_Release.zip&p_Doc_Ref=PM5760
PM5320, PM5340	V2.1.3 and earlier	A fix in V2.1.5 is now available for download: https://download.schneider-electric.com/files?p_enDocType=Firmware&p_File_Name=PM5320_PM5340_v2.1.5_HW_vB1.zip&p_Doc_Ref=PM5320_PM5340
PM5341	V2.4.1 and earlier	A fix in V2.4.4 is now available for download: https://download.schneider-electric.com/files?p_enDocType=Firmware&p_File_Name=PM5341_v2.4.4_HW_vB1.zip&p_Doc_Ref=PM5341

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 mobile devices 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 refer to the Schneider Electric Recommended Cybersecurity Best Practices document.

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, contact your local Schneider Electric representative or Schneider Electric Industrial Cybersecurity Services: https://www.se.com/ww/en/work/solutions/cybersecurity/. These organizations will be fully aware of this situation and can support you through the process.

For further information related to cybersecurity in Schneider Electric's products, visit the company's cybersecurity support portal page:
https://www.se.com/ww/en/work/support/cybersecurity/overview.jsp

For related information, refer to the Treck TCP/IP Vulnerabilities Security Bulletin:
https://www.se.com/ww/en/download/document/SESB-2020-168-01

Revision Control:

Version 1 *23 June 2020*	Original Release

Schneider Electric Security Notification

Version 1.1 *24 June 2020*	- Added link to related SEVD-2020-174-01 Security Notification document for Network Management Card (NMC) offers (pages 4-5) - Minor formatting changes
Version 1.2 *27 June 2020*	- Enhanced Andover Continuum affected product information (page 3) - Minor formatting changes
Version 1.3 *2 July 2020*	Added Acti9 Smartlink EL B to affected product list (page 2)
Version 1.4 *14 July 2020*	Removed Smartlink ELEC (duplicate reference for Acti9 Smartlink EL B) from the affected product list (page 3)
Version 2.0 *29 July 2020*	- Added *Wiser Energy IP module by Schneider Electric*, , *Wiser Energy IP module by Schneider Electric* , and *Gateway Connector by Elko* to affected products list (page 5) - Added *XUPH001 OsSense communication module* and *XGCS850C201 OsiSense RFID compact smart antenna* to affected products list (page 2) - Removed *PowerLogic EGX100*, *ECI850 Sepam IEC 61850 Server*, and *PowerLogic G3200 Modbus to IEC 61850 Gateway* from affected products list. (page 3)
Version 2.1 *5 August 2020*	Added remediation for *Uninterruptible Power Supply (UPS) using NMC2* (page 2)
Version 2.2 *6 August 2020*	Corrected affected version(s) and enhanced remediation/mitigation version details for *Uninterruptible Power Supply (UPS) using NMC2* (page 2)
Version 2.3 *1 September 2020*	Added remediation for *Cooling Products using NMC2* and partial remediations for *ATM3BC bus coupler module – EIP, TM3BC bus coupler module – SL, and TM3BC bus coupler module – CANOpen (page 2-3)*
Version 2.4 *13 October 2020*	Added remediation guidance for *VW3A3310 Altivar 61/71 Modbus TCP, VW3A3310D Altivar 61/71 Ethernet daisy chain, VW3A3316 Altivar 61/71 Ethernet IP*, and *VW3A3320 Altivar 61/71 Ethernet IP RSTP* options. *(page 2-3)*
Version 2.5 *23 October 2020*	- Added remediation for *EGX150/Link150 Ethernet Gateway , Acti9 PowerTag Link / HD , Acti9 Smartlink SI D , and Acti9 Smartlink SI B* - All APC Network Management Card related impact and remediation information has been moved to the existing Security Notification SEVD-2020-174-01 for increased clarity. - Added *PowerLogic EGX100* to affected products list • ***Note**: Based on information received earlier this year, Schneider Electric originally determined that its PowerLogic EGX100 was not affected by vulnerabilities in Treck Inc.'s embedded TCP/IP stack. After receiving additional information and analysis from Treck, Inc and JSOF, Schneider Electric has determined this offer is impacted. Users of this product are encouraged to apply the recommended mitigation actions immediately to*

	minimize the risks associated with vulnerabilities in Treck Inc.'s embedded TCP/IP stack.
Version 2.6 *10 November 2020*	Added remediations for *eIFE Ethernet Interface for MasterPact MTZ drawout circuit breakers*, *IFE Ethernet Interface for ComPact, PowerPact, and MasterPact circuit breakers*, and *IFE Gateway* (*page 4*)
Version 2.7 *8 December 2020*	Added remediations for *SCADAPack 32 RTU, XUPH001 OsSense communication module, XGCS850C201 OsiSense RFID compact smart antenna, ATV340E Altivar Machine Drives, ATV630/650/660/680/6A0/6B0 Altivar Process Drives, ATV930/950/960/980/9A0/9B0 Altivar Process Drives, VW3A3720, VW3A3721 Altivar Process Communication Modules, ACE850 Sepam communication interface, PowerLogic EGX300 Ethernet Gateway, PowerLogic EGX100 Ethernet Gateway, Acti9 Smartlink IP* (*page 2, 4-5*)
Version 2.8 *8 December 2020*	Added remediations for *EcoStruxure Building SmartX IP RP Controllers* and *EcoStruxure Building SmartX IP MP Controllers* (*page 6*)
Version 2.9 *12 January 2021*	Added remediations for PowerLogic PM5000 Series Power Meters in Download Links section (*page 11*)
Version 2.10 *9 March 2021*	Fixed version for *EcoStruxure Building SmartX IP MP Controllers* and *EcoStruxure Building SmartX IP RP Controllers* corrected to 3.02.02 (previously listed as 3.02.01) (*page 6*)
Version 2.11 *12 April 2021*	Added remediation for *Acti9 PowerTag Link C* (*page 5*)
Version 2.12 *11 May 2021*	Added remediation for *ZBRCETH Modbus TCP communication module for ZBRN1 Harmony Hub* (*page 4*)
Version 2.13 13 July 2021	Added remediation for *TM3 bus coupler modules – EIP/SL/CANOpen* and *Acti9 Smartlink EL B A9XELC08* (page 2-3, 5)
Version 2.14 10 Aug 2021	Corrected download links for *TM3 bus coupler modules – EIP/SL/CANOpen* (page 2-3)

Product Security Office

Digitally signed by Product Security Office
Date: 2021.08.10 09:37:08 -04'00'