Schneider Electric Security Notification

Treck TCP/IP Vulnerabilities (Ripple20) (V1.1)

23 June 2020 (24 June 2020)

Overview

Schneider Electric is aware of multiple vulnerabilities affecting Treck Inc.'s embedded TCP/IP stack, 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.

Affected Products

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

Industrial Automation Products	All versions
ATV340E Altivar Machine Drives	All Versions (V3.1IE23 and earlier)
ATV6000 Medium Voltage Altivar Process Drives	All Versions (V1.1IE02 and earlier)
ATV630/650/660/680/6A0/6B0 Altivar Process Drives	All Versions (V2.6IE31 and earlier)

ATV930/950/960/980/9A0/9B0 Altivar Process Drives	All Versions (V3.1IE24 and earlier)
SCADAPack 32 RTUs	All versions (V2.24 and earlier)
TM3BC bus coupler module - EIP	All Versions
TM3BC bus coupler module - SL	All Versions
TM3BC bus coupler module - CANOpen	All Versions
VW3A3310 Altivar 61/71 Modbus TCP option	All Versions (V2.1IE09 and earlier)
VW3A3310D Altivar 61/71 Ethernet daisy chain option	All Versions (V3.0IE11 and earlier)
VW3A3316 Altivar 61/71 Ethernet IP option	All Versions (V1.2IE14 and earlier)
VW3A3320 Altivar 61/71 Ethernet IP RSTP option	All Versions (V1.1IE19 and earlier)
VW3A3720, VW3A3721 Altivar Process Communication Modules	All Versions (V1.15IE18 and earlier)
ZBRCETH Modbus TCP communication module for ZBRN1 Harmony Hub	All Versions (V02.03 and earlier)
Energy Management Products	**Affected Version**
ACE850 Sepam communication interface	All versions
Acti9 PowerTag Link C	All versions
Acti9 PowerTag Link HD	All versions
Acti9 Smartlink IP	All versions
Acti9 Smartlink EL D	All versions
Acti9 Smartlink SI B	All versions
Acti9 Smartlink SI D	All versions
EcoStruxure Building SmartX IP MP Controllers	All versions
EcoStruxure Building SmartX IP RP Controllers	All versions

Continuum Net Controller 2 models: BCX1-CR-64-INF-X1 - BCX1-CR-64-INF - BCX1-CR-32-INF-X1 - BCX1-CR-32-INF - BCX1-CR-8-INF-X1 - BCX1-CR-8-INF-SA - BCX1-CR-8-INF - BCX1-CR-0-INF-X1 - BCX1-CR-0-INF-X2 - BCX1-CR-0-INF - BCX1-CR-127-INF	All versions
ECI850 Sepam IEC 61850 Server	All versions
PowerLogic EGX100, EGX300 Ethernet Gateways	All versions
EGX150/Link150 Ethernet Gateway	All versions
eIFE Ethernet Interface for MasterPact MTZ drawout circuit breakers	All versions
IFE Ethernet Interface for ComPact, PowerPact, and MasterPact circuit breakers	All versions
IFE Gateway	All versions
PowerLogic G3200 Modbus to IEC 61850 Gateway	All versions
PowerLogic PM5000 series power meters	All versions
Smartlink ELEC	All versions
TeSys T LTMR08EBD Motor Controller	All versions
Uninterruptible Power Supply (UPS)* See related Security Notification SEVD-2020-174-01 document. **Smart-UPS and Symmetra UPS Network Management Card 1 (NMC1) SmartSlot Models:** - AP9617 (discontinued in Nov 2011) - AP9619 (discontinued in Sep 2012) - AP9618 (discontinued in Jan 2017)	NMC1: AOS V3.9.2 and earlier NMC2: AOS V6.8.8 and earlier NMC3: AOS V1.3.0.6 and earlier

- Audio/Video Network Management Enabled products • S20BLK, G50NETB2, G50NETB-20A2 **Smart-UPS, Symmetra, and Galaxy UPS with the following NMC2 SmartSlot models:** - AP9630/AP9630CH/AP9630J - AP9631/AP9631CH/AP9631J - AP9635/AP9635CH **Network Management Card 3 (NMC3) SmartSlot card models:** - AP9640/AP9640J - AP9641/AP9641J	
APC Rack Power Distribution Units (PDU)* See related Security Notification SEVD-2020-174-01 document. Embedded NMC1: - Metered/Switched Rack PDUs with embedded NMC1 - AP78XX, AP79XX Embedded NMC2: - 2G Metered/Switched Rack PDUs with embedded NMC2 - AP84XX, AP86XX, AP88XX, AP89XX	NMC1: AOS V3.9.2 and earlier NMC2: AOS V6.8.8 and earlier
Battery Management* See related Security Notification SEVD-2020-174-01 document. Embedded NMC1 - Battery Management System - AP9921X Embedded NMC2 - Battery Manager - AP9922	NMC1: AOS V3.9.2 and earlier NMC2: AOS V6.8.8 and earlier
Rack Automatic Transfer Switches (ATS)* See related Security Notification SEVD-2020-174-01 document. Embedded NMC1 - Rack Automatic Transfer Switches - AP77XX	NMC1: AOS V3.9.2 and earlier NMC2: AOS V6.8.8 and earlier

Embedded NMC2 - Rack Automatic Transfer Switches - AP44XX	
Environmental Monitoring* See related Security Notification SEVD-2020-174-01 document. Embedded NMC1 - AP9320 - AP9340 - AP9361 - NetBotz NBRK0200 Embedded NMC2 - NetBotz NBRK0250	NMC1: AOS V3.9.2 and earlier NMC2: AOS V6.8.8 and earlier
Cooling Products* See related Security Notification SEVD-2020-174-01 document. Embedded NMC1 - NetworkAir - InRow Embedded NMC2 & Touchscreen Displays: - InRow - Uniflair Cooling Devices	NMC1: AOS V3.9.2 and earlier NMC2: AOS V6.8.8 and earlier
***includes but may not be limited to the specific affected offer examples listed**	

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.

Schneider Electric Security Notification

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 and/or Schneider Electric Industrial Cybersecurity Services. These organizations will be fully aware of this situation and can support you through the process.

https://www.se.com/ww/en/work/support/cybersecurity/overview.jsp

https://www.se.com/ww/en/work/services/field-services/industrial-automation/industrial-cybersecurity/industrial-cybersecurity.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

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 Security Notification

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 *23 June 2020*	Original Release
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

Product Security Office

Digitally signed by Product Security Office
Date: 2020.06.23 18:56:09 -04'00'