Schneider Electric Security Notification

Treck TCP/IPv6 Vulnerabilities (V4.0)

18 December 2020 (14 September 2021)

Overview

Schneider Electric is aware of multiple vulnerabilities affecting the IPv6 option in Treck Inc.'s embedded TCP/IP stack, which can be found in a variety of embedded devices and in varying forms (compiled, included and as a linked library). Treck's TCP/IP stack is implemented and has been adopted in a wide variety of industries, including medical, industrial controls and IoT applications. Therefore, these vulnerabilities have wide-ranging impact across multiple IT and industrial segments.

Schneider Electric continues to assess how these newly disclosed vulnerabilities affect its offers. The vulnerabilities range in severity and therefore have varying levels of risk. The company will 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 mitigation recommendations below.

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

September 2021 Update: Added remediations for Acti9 Smartlink SI D and EGX150/Link150 Ethernet Gateway

Vulnerability Details

CVE ID: CVE-2020-27337

CVSS v3.1 Base Score 7.3 | High | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

A CWE-787: Out-of-bounds Write vulnerability exists that could cause improper input validation in the ICMPv6 component when handling a packet sent by a remote attacker.

CVE ID: CVE-2020-27338

CVSS v3.1 Base Score 5.9 | Medium | CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:H

A CWE-125: Out-of-bounds Read vulnerability exists that could cause improper input validation in the DHCPv6 component when handling a packet sent by a remote attacker.

Schneider Electric Security Notification

CVE ID: CVE-2020-27336

CVSS v3.1 Base Score 3.7 | Low | CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N

A CWE-125: Out-of-bounds Read vulnerability exists that could cause improper input validation in the IPv6 component when handling a packet sent by a remote attacker.

Affected Products & Remediations

Schneider Electric has determined that the following offers are impacted. This notification will be updated as remediations become available. For all other affected products, customers should refer to the recommended mitigations to reduce risk to their installations.

Please subscribe to the Schneider Electric security notification service to be informed of critical updates to this notification: https://www.se.com/ww/en/work/support/cybersecurity/security-notifications.jsp

Available Remediations

Products	Affected Version	Remediation/Mitigation
Acti9 Powertag Link/HD	Version 002.000.006 and prior	Customers should update firmware using EcoStruxure Power Commission (EPC) installer v.7.0 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	Version 002.004.002 and prior	Customers should update firmware using EcoStruxure Power Commission (EPC) installer v.7.0 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	All versions	Acti9 Smartlink SI D as reached its end of life and is no longer supported. Customers should immediately apply the following mitigations to reduce the risk of exploit: • *Disable IPv6 service in the product configuration* It is also recommended to replace "Acti9 Smartlink SI D" by the latest "Acti9 PowerTag Link" offering to resolve this issue.
ATV340E Altivar Machine Drives	All versions prior to V3.2IE25	A fix is now available in product releases V3.2IE25 and above. For versions released 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 available in product releases V3.3IE33 and above. For versions released 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 available in product releases V3.3IE26 and above. For versions released prior V3.3IE26, apply the mitigations detailed in the Recommended Mitigations section and contact your local technical support for more information.
EGX150/Link150 Ethernet Gateway**	All versions prior V5.1.24	A fix is available on V5.1.24 available for download at: https://download.schneider-electric.com/files?p_enDocType=Firmware&p_File_Name=005.001.024.zip&p_Doc_Ref=FW_v5.1.24
TM3 Bus Coupler EIP	All versions prior to V2.2.1.1	A fix is available in firmware version V2.2.1.1 which can be downloaded below: https://www.se.com/ww/en/download/document/TM3BC_EIP_2_2_1_1/

VW3A3720, VW3A3721 Altivar Process Communication Modules	All versions prior to V1.15IE25	A fix is now available in product releases V1.15IE25 and above. For versions released prior V1.15IE25, apply the mitigations detailed in the Recommended Mitigations section and contact your local technical support for more information.
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).	All versions prior to AOS V6.9.6	A fix is now available in product releases with AOS V6.9.6 and later. Contact your local technical support for more information on firmware availability.
APC Network Management Card 3 (NMC3) - AP9640, AP9641	All versions prior to AOS V1.4.0	A fix is now available in product releases with AOS V1.4.0 and above. Contact your local technical support for more information on firmware availability.

*** Note the CVSS score for CVE-2020-27337 is evaluated as Medium in the product context as it is only accessible via link-local segment*

Affected Products

Products	Affected Version
ATV6000 Medium Voltage Altivar Process Drives	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

Acti9 Smartlink IP*	All versions

** Product Specific Mitigations: Disable IPv6 service in the product configuration, or to reduce the risk of exploitation, apply the mitigations detailed in the Recommended Mitigations section. Note the CVSS score for CVE-2020-27337 is evaluated as Medium in the product context as it is only accessible via link-local segment.*

*** Note the CVSS score for CVE-2020-27337 is evaluated as Medium in the product context as it is only accessible via link-local segment.*

Recommended Mitigations

Since the vulnerabilities are present in the IPv6 function of the TCP/IP stack, an active IPv6 network interface 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 ICMPv6, DHCPv6, IPv6 traffic and malformed packets.
- Ensure that embedded and critical devices are not accessible from the Internet, unless absolutely essential, and then always minimize their network exposure.

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 Schneider Electric representative or local technical support.

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. 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

Schneider Electric Security Notification

RESULT FROM YOUR USE OF THIS NOTIFICATION. 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 1.0 *18 December 2020*	Original Release
Version 2.0 *13 July 2021*	Added remediation for *Acti9 Powertag Link/HD* and *Acti9 Smartlink SI B*. (page 2)
Version 3.0 *10 August 2021*	Added remediation for TM3 Bus Coupler EIP
Version 4.0 *14 September 2021*	Added remediations for Acti9 Smartlink SI D and EGX150/Link150 Ethernet Gateway

Product Security Office

Digitally signed by Product Security Office
Date: 2021.09.10 17:09:12 -04'00'