Schneider Electric Security Notification

Treck HTTP Server Vulnerability on TM3 Bus Coupler Modules (V2.0)

18 December 2020 (10 August 2021)

Overview

Schneider Electric is aware of a vulnerability affecting Treck Inc.'s HTTP Server component used in the Schneider Electric TM3BC bus coupler modules.

Failure to apply the mitigations provided below may risk heap-based buffer overflow, which could result in Denial of Service of the webserver.

August 2021 Update: Added remediation for all TM3 Bus Coupler products.

Affected Products and Versions

- TM3 Bus Coupler – EIP firmware version 2.1.50.2 and prior
- TM3 Bus Coupler – SL firmware version 2.0.50.2 and prior
- TM3 Bus Coupler – CANOpen firmware version 2.0.50.2 and prior

All TM3 Bus Coupler modules have a USB RNDIS port, which allows for Ethernet communications over USB. Because of the nature of the EIP protocol, the TM3BC EIP is the only version with an Ethernet adaptor.

Vulnerability Details

CVE ID: **CVE-2020-25066**

CVSS v3.1 Base Score 10 | Critical | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

A heap-based buffer overflow in the Treck HTTP Server component before 6.0.1.68 allows remote attackers to cause a denial of service (crash/reset) or to possibly execute arbitrary code.

Remediation

Affected Product & Version	Remediation
TM3 Bus Coupler – EIP	A fix is now 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/
TM3 Bus Coupler – SL	A fix is now available in firmware version V2.1.1.1 which can be downloaded below: https://www.se.com/ww/en/download/document/TM3BC_MBSL_2_1_1_1/

TM3 Bus Coupler – CANOpen	A fix is now available in firmware version V2.1.1.1 which can be downloaded below: https://www.se.com/ww/en/download/document/TM3BC_CO_2_1_1_1/

Customers should use appropriate patching methodologies when applying these patches to their systems. We strongly recommend the use of back-ups and evaluating the impact of these patches in a Test and Development environment or on an offline infrastructure. Contact Schneider Electric's Customer Care Center if you need assistance removing a patch.

If customers choose not to apply the remediation provided above, they should immediately apply the following mitigations to reduce the risk of exploit:

- Restrict physical access to the USB RNDIS port of the Bus Coupler
- Prevent permanent connection between the engineering workstation and the USB RNDIS port of the Bus Coupler, so that no unauthorized personnel or device can access your product.
- Minimize network exposure, keeping exposure to the minimum necessary, and ensuring that devices are not accessible from the Internet.
- Implement a firewall to block all unauthorized access to ports 80/TCP and 443/TCP.
- If network access is not required: Remove the Ethernet cable from the affected device.

To ensure you are informed of all updates, including details on affected products and remediation plans, please subscribe to Schneider Electric's security notification service here:

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

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 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.

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

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.

Schneider Electric Security Notification

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 *10 August 2021*	Added remediation for all TM3 Bus Coupler products.

Product Security Office

Digitally signed by Product Security Office
Date: 2021.08.10 09:19:25 -04'00'