# Schneider Electric Security Bulletin

## Treck TCP/IP Vulnerabilities (Ripple20) (V2.0)

**17 June 2020 (23 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. In the meantime, customers should immediately ensure they have implemented cybersecurity best practices across their operations to protect themselves from 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 recommended mitigations and general security recommendations below.

Refer to the Treck TCP/IP Vulnerabilities Security Notification for offer specific information: https://www.se.com/ww/en/download/document/SEVD-2020-175-01

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

## Vulnerability Details

Treck has disclosed 19 different vulnerabilities existing in its TCP/IP stack. These vulnerabilities range in severity and at least two could lead to remote code execution. Other potential impacts of these vulnerabilities include privilege escalation, denial of service, and information leakage.

- 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.

## Recommended Mitigations

For recommended mitigations, please review the Treck TCP/IP Vulnerabilities Security Notification: https://www.se.com/ww/en/download/document/SEVD-2020-175-01

## 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 it is intended for.
- Scan all methods of mobile data exchange with the isolated network such as CDs, USB drives, etc. before use in 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.

## More Information

This document is intended to help provide an overview of the identified situation and actions required to mitigate it.

To obtain full details on the issues and assistance on how to protect your installation, contact your local Schneider Electric representative or your Customer Care Center: https://www.se.com/us/en/work/support/contacts.jsp. These organizations are fully aware of the 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

# Schneider Electric Security Bulletin

If you require additional support, Schneider Electric Industrial Cybersecurity Services team is available to help. Visit: https://www.se.com/ww/en/work/solutions/cybersecurity/

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 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.

## 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 digital automation** 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 unleashing the infinite possibilities of an **open, global, innovative community** that is passionate about our **Meaningful Purpose, Inclusive and Empowered** values.

www.se.com

Revision Control:

| | |
|---|---|
| **Version 1.0**<br>*17-Jun-2020* | Original Release |
| **Version 2.0**<br>*22-Jun-2020* | • Updated Overview Section to provide link to Security Notification (page 1)<br>• Updated Recommended Mitigations section (page 2) |

Product Security Office

Digitally signed by Product Security Office
Date: 2021.02.23 13:08:42 -05'00'