Schneider Electric Security Bulletin

Trio Q and J Data Radios

10 November 2020

Overview

Schneider Electric is aware of the recently published Drovorub malware. To further mitigate the effects of this malware, Schneider Electric recommends applying a defense in depth approach to protect their Q Data Radio and J Data Radio devices from malware being installed. In addition, Schneider Electric recommends customers make use of the available features to reduce the risk of malware installation such as user access controls and the available secure protocols HTTPS and SSH.

Details

The Trio Q Data Radio products and Trio J Data Radio products are ethernet and serial data radios that provide long range wireless data communications in SCADA and remote telemetry applications.

Failure to apply the recommended mitigations provided below may put a user of these devices at risk of being attacked by the Drovorub malware, which, in turn, could result in an attacker gaining direct communications capability with actor-controlled command and control infrastructure, file download and upload capabilities, execution of arbitrary commands, port forwarding of network traffic to other hosts on the network, and implements a hiding techniques to evade detection. All effective defenses if the attacker is first able to gain root privileges through another vulnerability.

See the NSA fact sheet on Drovorub for more details:

https://www.nsa.gov/Portals/70/documents/resources/cybersecurity-professionals/DROVORUB-Fact%20sheet%20and%20FAQs.pdf?ver=2020-08-13-114246-203

Recommended Mitigations

Schneider Electric is establishing a remediation plan for all future versions of Trio J-Series Data Radios and Trio Q-Series Data Radios that will include a fix for the Drovorub vulnerability. We will update this document when the remediation is available. Until then, customers should immediately apply the following mitigations to reduce the risk of exploit:

Enable Role-Based Access Control (RBAC). Instructions can be found here:

Trio Q Data Radio User Manual Section 8.5.1 Centralized User Access Control, page 254

Trio J Series Ethernet User Manual Part F Quick Reference Guide, page 60

Schneider Electric Security Bulletin

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 following industry cybersecurity best practices such as:

- Enable user access control
- Use SSH or HTTPS and avoid Telnet or HTTP
- 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.
- 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 Bulletin

LEGAL DISCLAIMER

THIS NOTIFICATION DOCUMENT, THE INFORMATION CONTAINED HEREIN, AND ANY MATERIALS LINKED FROM IT (COLLECTIVELY, THIS "NOTIFICATION") ARE 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 OR GUARANTEE OF ANY KIND. SCHNEIDER ELECTRIC DISCLAIMS ALL WARRANTIES RELATING TO THIS NOTIFICATION, EITHER EXPRESS OR IMPLIED, INCLUDING WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SCHNEIDER ELECTRIC MAKES NO WARRANTY THAT THE NOTIFICATION WILL RESOLVE THE IDENTIFIED SITUATION. IN NO EVENT SHALL SCHNEIDER ELECTRIC BE LIABLE FOR ANY DAMAGES OR LOSSES WHATSOEVER IN CONNECTION WITH THIS NOTIFICATION, 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. YOUR USE OF THIS NOTIFICATION IS AT YOUR OWN RISK, AND YOU ARE SOLELY LIABLE FOR ANY DAMAGES TO YOUR SYSTEMS OR ASSETS OR OTHER LOSSES THAT MAY 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 *10 November 2020*	Original Release

Product Security Office

Digitally signed by Product Security Office
Date: 2020.11.08 20:22:18 -05'00'