

Schneider Electric Security Notification

Trio™ Q Licensed Data Radios

8 April 2025

Overview

Schneider Electric is aware of a vulnerability in its Trio™ Q Licensed Data Radio product.

The [Trio Q Licensed Data Radios](#) product is an advanced, high-speed licensed digital data radios, providing both Ethernet and serial communications for complex and demanding applications in Point-to-Point Multipoint (Multiple Address Radio) Telemetry and remote SCADA Systems.

Failure to apply the remediations or mitigations provided below may risk disclosure of information that could result in unauthorized access, loss of confidentiality, integrity, and availability of the product.

Affected Products and Versions

Product	Version
Trio™ Q Licensed Data Radio	Versions prior to v2.7.2

Vulnerability Details

CVE ID: **CVE-2025-2440**

CVSS v3.1 Base Score 4.2 | Medium | CVSS:3.1/AV:P/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N

CVSS v4.0 Base Score 4.1 | Medium | CVSS:4.0/AV:P/AC:H/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N

CWE-922: Insecure Storage of Sensitive Information vulnerability exists that could potentially lead to unauthorized access of confidential data when a malicious user, having physical access and advanced information on the file system, sets the radio in factory default mode.

CVE ID: **CVE-2025-2441**

CVSS v3.1 Base Score 4.6 | Medium | CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

CVSS v4.0 Base Score 4.1 | Medium | CVSS:4.0/AV:P/AC:L/AT:P/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N

CWE-1188: Initialization of a Resource with an Insecure Default vulnerability exists that could lead to loss of confidentiality when a malicious user, having physical access, sets the radio in factory default mode where the product does not correctly initialize all data.

Schneider Electric Security Notification

CVE ID: **CVE-2025-2442**

CVSS v3.1 Base Score 6.8 | Medium | CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v4.0 Base Score 5.4 | Medium | CVSS:4.0/AV:P/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

CWE-1188: *Initialization of a Resource with an Insecure Default* vulnerability exists that could potentially lead to unauthorized access which could result in the loss of confidentiality, integrity and availability when a malicious user, having physical access, sets the radio to the factory default mode.

Note regarding vulnerability details: The severity of vulnerabilities was calculated using the CVSS Base metrics for 3.1 ([CVSS v3.1](#)). CVSS v3.1 will be still evaluated until the adoption of CVSS v4.0 by the industry. The severity was calculated without incorporating the Threat and Environmental metrics. Schneider Electric recommends that customers score the CVSS Environmental metrics, which are specific to end-user organizations, and consider factors such as the presence of mitigations in that environment. Environmental metrics may refine the relative severity posed by the vulnerabilities described in this document within a customer's environment.

Remediation

Affected Product & Version	Remediation
TRIO™ Q Data Radio Versions prior to v2.7.2	<p>Version v2.7.2 of the TRIO™ Q Data Radio firmware includes fixes for the identified vulnerabilities and is available for download here: https://www.se.com/ww/en/product-range/61419-trio-licensed-radios/#software-and-firmware</p> <p>Instructions should be followed from Section 10 Part J – Firmware Updating and Maintenance in the Trio Q Series Data Radio User Manual</p> <p>This section provides information on how to download, install, and verify the new firmware version.</p>

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:

Schneider Electric Security Notification

Mitigations

Affected Product & Version	Mitigations
TRIO™ Q Data Radio <i>Versions prior to v2.7.2</i>	<ul style="list-style-type: none">• Trio™ Data Radios should be installed in a secure location to prevent physical access by unauthorized personnel and securely disposed when decommissioned.• Firmware loaded in Trio™ Data Radios should be confirmed using the hash published with the release notes and following the instructions in Section 10 Part J – Firmware Updating and Maintenance in the Trio Q Series Data Radio User Manual This section provides information on how to download, install, and verify the new firmware version.

To ensure you are informed of all updates, including details on affected products and remediation plans, 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 intended for that device.
- 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.

Schneider Electric Security Notification

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:

<https://www.se.com/ww/en/work/solutions/cybersecurity/>. These organizations will be fully aware of this 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>

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

Schneider's purpose is to **create Impact** by empowering all **to make the most of our energy and resources**, bridging progress and sustainability for all. We call this Life Is On.

Our mission is to be the trusted partner in **Sustainability and Efficiency**.

We are a **global industrial technology leader** bringing world-leading expertise in electrification, automation and digitization to smart **industries**, resilient **infrastructure**, future-proof **data centers**, intelligent **buildings**, and intuitive **homes**. Anchored by our deep domain expertise, we provide integrated end-to-end lifecycle AI enabled Industrial IoT solutions with connected products, automation, software and services, delivering digital twins to enable profitable growth **for our customers**.

We are a **people company** with an ecosystem of 150,000 colleagues and more than a million partners operating in over 100 countries to ensure proximity to our customers and stakeholders. We embrace **diversity and inclusion** in everything we do, guided by our meaningful purpose of a **sustainable future for all**.

www.se.com

Schneider Electric Security Notification

Revision Control:

Version 1.0.0 08-Apr-25	Original Release
-----------------------------------	------------------