Schneider Electric Security Notification

Trio™ Licensed and License-free Data Radios

12 December 2023 (9 April 2024)

Overview

Schneider Electric is aware of multiple vulnerabilities in its Trio Licensed and License-Free Data Radio products.

The Trio Licensed Radio products are designed to provide complete, versatile, and high availability system solutions for long range wireless data communications in SCADA and remote telemetry applications. The Trio License-Free Radio products are a range of frequency-hopping Ethernet and Serial Data Radios operating in the license-free 900Mhz and 2.4 Ghz band and designed with versatility and flexibility in mind.

Failure to apply the remediations and mitigations provided below may risk disclosure of information, or potential installation of malicious code.

April 2024 Update: A remediation is now available for Trio J-Series Ethernet Data Radio on CVE-2023-5629.

Affected Products and Versions

Product	CVE-2023-5629	CVE-2023-5630
Trio E-Series Ethernet Data Radio	All versions in the models: ER45e, EB45e, EH45e	All Versions
Trio J-Series Ethernet Data Radio	Versions prior to 3.8.3	All Versions
Trio Q-Series Ethernet Data Radio	Versions prior to 2.7.0	All Versions

Vulnerability Details

CVE ID: **CVE-2023-5629**

CVSS v3.1 Base Score 8.2 | High | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:N

CWE-601: URL Redirection to Untrusted Site ('Open Redirect') vulnerability exists that could cause disclosure of information through phishing attempts over HTTP.

Schneider Electric Security Notification

CVE ID: **CVE-2023-5630**

CVSS v3.1 Base Score 6.5 | Medium | CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:H

CWE-494: Download of Code Without Integrity Check vulnerability exists that could allow a privileged user to install an untrusted firmware.

Note regarding vulnerability details: The severity of vulnerabilities was calculated using the CVSS Base metrics in version 3.1 (CVSS v3.1) without incorporating the Temporal 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	CVEs
Trio J-Series Data Radio *Versions prior to v3.8.3*	Version 3.8.3 of Trio J-Series Data Radio firmware includes a fix for vulnerability CVE-2023-5629 and is available for download here: https://www.se.com/us/en/product-range/61420-trio-licensefree-radios#software-and-firmware Instructions should be followed from Section 9 Part I – Firmware Updating and Maintenance in the Trio J Series Data Radio User Manual, available here: https://download.schneider-electric.com/files?p_Doc_Ref=Trio_JSeries_User_Manual&p_enDocType=User+guide&p_File_Name=Trio+J-Series+Ethernet+Data+Radio+User+Manual.pdf This section provides information on how to download, install, and verify the new firmware version.	CVE-2023-5629
Trio Q-Series Data Radio *Versions prior to v2.7.0*	Version 2.7.0 of Trio Q-Series Data Radio firmware includes a fix for vulnerability CVE-2023-5629 and is available for download here: https://www.se.com/us/en/download/document/TrioQFirmware/ Instructions should be followed from Section 10 Part J – Firmware Updating and Maintenance in the Trio Q Data Radio User Manual, available here:	CVE-2023-5629

	https://download.schneider-electric.com/files?p_Doc_Ref=Trio+Q+Data+Radio+User+Manual&p_enDocType=User+guide&p_File_Name=Trio+Q+Data+Radio+User+Manual.pdf This section provides information on how to download, install, and verify the new firmware version.	

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.

Mitigations

Affected Product & Version	Mitigations	CVEs
Trio Q-Series Data Radio *Versions prior to v2.7.0* **Trio E-Series Ethernet Data Radio** *All versions in the models: ER45e, EB45e, EH45e* **Trio J-Series Ethernet Data Radio** *Versions prior to v3.8.3*	Customers should only use up to date browsers, to access the login page for Trio E and Q Series radios. These browsers automatically prevent "Open Redirect" HTTP attempts. Note: Trio E-Series Ethernet Data Radio product has reached its end of life and is no longer supported. Customers should immediately apply the above mitigations to reduce the risk of exploit.	CVE-2023-5629
Trio Q-Series Data Radio *All Versions* **Trio E-Series Ethernet Data Radio** *All Versions*	Trio Data Radios should be installed in a secure location to prevent physical access by unauthorized personnel, and appropriate password protections put in place to prevent remote access by unauthorized personnel. 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 Data Radio User Manual, available here:	CVE-2023-5630

	https://download.schneider-electric.com/files?p_Doc_Ref=Trio+Q+Data+Radio+User+Manual&p_enDocType=User+guide&p_File_Name=Trio+Q+Data+Radio+User+Manual.pdf This section provides information on how to download, install, and verify the new firmware.	
Trio J-Series Ethernet Data Radio *All versions*	Trio Data Radios should be installed in a secure location to prevent physical access by unauthorized personnel, and appropriate password protections put in place to prevent remote access by unauthorized personnel. Firmware loaded in Trio Data Radios should be confirmed using the hash published with the release notes and following the instructions in Section 9 Part I – Firmware Updating and Maintenance in the Trio J Data Radio User Manual, available here: https://download.schneider-electric.com/files?p_Doc_Ref=Trio_JSeries_User_Manual&p_enDocType=User+guide&p_File_Name=Trio+J-Series+Ethernet+Data+Radio+User+Manual.pdf This section provides information on how to download, install, and verify the new firmware.	CVE-2023-5630

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.

Acknowledgements

Schneider Electric recognizes the following researcher for identifying and helping to coordinate a response to these vulnerabilities:

CVE	Researcher
CVE-2023-5629 CVE-2023-5630	The UK's National Cyber Security Centre (NCSC)

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

Schneider Electric Security Notification

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 empower 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 your digital partner for Sustainability and Efficiency.

We drive digital transformation by integrating world-leading process and energy technologies, end-point to cloud connecting products, controls, software and services, across the entire lifecycle, enabling integrated company management, for homes, buildings, data centers, infrastructure and industries.

We are the most local of global companies. We are advocates of open standards and partnership ecosystems that are passionate about our shared Meaningful Purpose, Inclusive and Empowered values.
www.se.com

Revision Control:

Version 1.0.0 *12 December 2023*	Original Release
Version 2.0.0 *09 April 2024*	A remediation is now available for Trio J-Series Ethernet Data Radio on CVE-2023-5629.

CPCERT

Digitally signed by CPCERT
Date: 2024.04.08 10:06:35 -04'00'