Overview

Schneider Electric® has become aware of a vulnerability involving the Trio J-Series License Free Ethernet Radio when the device has AES encryption enabled.

Vulnerability Overview

Trio J-Series Radio Firmware Versions V3.6.0, V3.6.1, V3.6.2 and V3.6.3 do not correctly generate an AES encryption key when AES encryption is enabled in the device configuration.

Product(s) Affected

The following products are affected by the Trio J-Series Radio Encryption Key vulnerability:

TBURJR900-00002DH0
TBURJR900-01002DH0
TBURJR900-05002DH0
TBURJR900-06002DH0
TBURJR900-00002EH0
TBURJR900-01002EH0
TBURJR900-05002EH0
TBURJR900-06002EH0

Running Firmware Versions V3.6.0, V3.6.1, V3.6.2 and V3.6.3

Vulnerability Details

- Trio J-Series Radio Firmware Versions V3.6.0, V3.6.1, V3.6.2 and V3.6.3 do not correctly generate an AES encryption key when AES encryption is enabled in the device configuration.
- When AES encryption is enabled, an encryption key is generated by the product (based on the user configured pass phrase)
- When AES encryption is enabled with these firmware versions, a key is generated incorrectly.

- If AES encryption was enabled in a Trio J-Series Radio running firmware version V3.5.0 or earlier, and the device was later upgraded to V3.6 (as noted above), AES encryption operates correctly and the system is not vulnerable
- If a Trio J-Series Radio running firmware version V3.5.0 or earlier was:
    - upgraded to V3.6 (as noted above), and
    - had AES encryption already enabled, and
    - no changes were made to the AES encryption pass phrase,

  then the Trio J-Series will continue to operate correctly

- If a Trio J-Series Radio running firmware version V3.5.0 or earlier was:
    - upgraded to V3.6 (as noted above), and
    - had AES encryption changed from disabled to enabled OR
    - had the AES encryption key changed

  then the unit will generate an invalid key

Schneider Electric has been designing industrial automation products for many years; Schneider Electric follows, and recommends to its customers, industry best practices in the development and implementation of control systems. This recommendation includes a Defense in Depth approach to secure an Industrial Control System.

Download our Cybersecurity whitepaper from www.schneider-electric.com. See Support > Cybersecurity

Schneider Electric takes these vulnerabilities very seriously and we have devoted resources to immediately investigate and address these issues. We believe it is critical to consider the whole picture, including safety, security and reliability. Any patches/solutions/mitigations we release will be carefully tested to ensure that they can be deployed in a manner that is both safe and secure.

CVSS Scoring

CVSS scores are a standard way of ranking vulnerabilities and are provided for reference based on a typical control system they should be adapted by individual users as required.

CVSS Base Score: 8.3, the vector is (AV:A/AC:L/Au:N/C:C/I:C/A:C)

Mitigation

Schneider Electric has fixed this issue in released firmware for the Trio J-Series License Free Ethernet Radio in Firmware Version V3.6.4 and later.

Updated firmware can be obtained from the Schneider Electric global website. Alternatively, contact your local Schneider Electric office to obtain the latest firmware for Trio J-Series range of products. For technical support please contact supportTRSS@schneider-electric.com

After performing an upgrade to V3.6.4 or later, activate a factory default reset, then reconfigure the radio and re-enable AES encryption. Details on how to perform firmware upgrades and factory default resets can be found in the J-Series User Manual or Quick Start Guides available for download from the Schneider Electric global website.

For More Information

This document is intended to help provide an overview of the identified vulnerability and actions required to mitigate it. To obtain full details on the issues and assistance on how to protect your installation, please contact your local Schneider Electric representative. These organizations will be fully aware of the situation and can support you through the process.

For further information on vulnerabilities in Schneider Electric's products, please visit Schneider Electric's cybersecurity web page at http://www2.schneider-electric.com/sites/corporate/en/support/cybersecurity/cybersecurity.page

About Schneider Electric

As a global specialist in energy management with operations in more than 100 countries, Schneider Electric offers integrated solutions across multiple market segments, including leadership positions in Utilities & Infrastructures, Industries & Machine Manufacturers, Non-residential Buildings, Data Centers & Networks and in Residential.
www.schneider-electric.com