PHOENIX CONTACT GmbH & Co. KG
Flachsmarktstraße 8
32825 Blomberg, Germany
Telefon: +49 5235 300
Telefax: +49 5235 3-41200
Internet: http://www.phoenixcontact.com
USt-Id-Nr.: DE124613250
WEEE-Reg.-Nr.: DE50738265

PHOENIX CONTACT GmbH & Co. KG · 32825 Blomberg

11 May 2022
300545335

Security Advisory for RAD-ISM-900-EN-BD devices

Advisory Title

Multiple vulnerabilities have been discovered in the firmware and in libraries utilized of RAD-ISM-900-EN-BD devices.

Advisory ID

CVE-2022-29897
CVE-2022-29898
VDE-2022-018

Vulnerability Description

RCE via Traceroute Utility:
A vulnerability was discovered that allows an attacker to execute arbitrary shell commands via the traceroute function found on the device's web application. This is achieved by exploiting the devices lack of input validation (CWE-20).

RCE and Unrestricted File Upload via Configuration Uploader:
A vulnerability was discovered that allows an attacker to execute arbitrary shell and/or upload arbitrary files to the device. This is achieved through bypassing the devices integrity detection mechanisms (CWE-354).

Vulnerabilities related to outdated libraries:

- BusyBox version 0.60.1: A CVE scan revealed 13 potential vulnerabilities. Some of these vulnerabilities impact services used by this device such as NTP and DHCP.
- OpenSSL version 0.9.7-beta3: This version of OpenSSL uses deprecated ciphers and a CVE scan revealed over 87 potential vulnerabilities.

Over-privileged web application:
The web application is operated with root privileges. Therefore, if an attacker were able to achieve RCE via the web application they would be executing with the highest level of privileges.

Affected products

Article no	Article	Affected versions
2901205	RAD-ISM-900-EN-BD/B	All versions
2900016	RAD-ISM-900-EN-BD	All versions
2900017	RAD-ISM-900-EN-BD-BUS	All versions

Impact

The abovementioned vulnerabilities allow an attacker to execute arbitrary shell commands and/or upload arbitrary files to the device with root privileges.

Some software libraries compiled into the device firmware are outdated and contain known vulnerabilities. Some of those vulnerabilities may be exploitable in the device context whilst others may not have any effect as the specific vulnerable function is not used. These vulnerabilities have not been investigated in detail.

Classification of Vulnerability

CVE-2022-29897
Base Score: 9.1
Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H
CWE-20: Improper Input Validation
https://nvd.nist.gov/vuln/detail/CVE-2022-29897

CVE-2022-29898
Base Score: 9.1
CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H
CWE-354: Improper Validation of Integrity Check Value
https://nvd.nist.gov/vuln/detail/CVE-2022-29898

CVE score and vector may have changed since publication of this advisory. You can find the current rating of a CVE at the respective link to the NVD website provided above.

Temporary Fix / Mitigation

Phoenix Contact recommends operating network-capable devices in closed networks or protected with a suitable firewall. For detailed information on our recommendations for measures to protect network-capable devices, please refer to our application note:

Measures to protect network-capable devices with Ethernet connection

Remediation

The family of RAD-ISM-900-EN-BD devices is end of life and will not receive updates anymore. If operation within a secured environment cannot be ensured in the specific customer application, please contact your local PHOENIX CONTACT support to discuss alternative solutions.

Acknowledgement

These vulnerabilities were discovered and reported by Logan Carpenter of DRAGOS.
We kindly appreciate the coordinated disclosure of this vulnerability by the finder.

PHOENIX CONTACT thanks CERT@VDE for the coordination and support with this publication.