SSA-856721: Vulnerability in RUGGEDCOM Discovery Protocol (RCDP) of Industrial Communication Devices

Publication Date:	2017-09-28
Last Update:	2018-02-22
Current Version:	V1.2
CVSS v3.0 Base Score:	8.8

SUMMARY

The RUGGEDCOM RCDP protocol is not properly configured after commissioning of RUGGEDCOM ROS based devices and some SCALANCE X switch models and could allow unauthenticated remote users to perform administrative operations. An attacker must be in the same adjacent network and the RCDP daemon must be enabled in order to exploit the vulnerability.

Siemens has released updates for all affected products and recommends that customers update to the new versions.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
RUGGEDCOM ROS for RSL910 devices: All versions < ROS V5.0.1	Install V5.0.1 The firmware updates for the Ruggedcom ROS-based devices can be obtained for free by contacting the Siemens support team at: https://support.industry.siemens.com/my/us/en/requests#createRequest
RUGGEDCOM ROS for all other devices: All versions < ROS V4.3.4	Install V4.3.4 The firmware updates for the Ruggedcom ROS-based devices can be obtained for free by contacting the Siemens support team at: https://support.industry.siemens.com/my/us/en/requests#createRequest
SCALANCE XB-200/XC-200/XP-200/XR300-WG: All versions between V3.0 (including) and V3.0.2 (excluding)	Install V3.0.2 https://support.industry.siemens.com/cs/de/en/view/109754174
SCALANCE XR-500/XM-400: All versions between V6.1 (including) and V6.1.1 (excluding)	Install V6.1 https://support.industry.siemens.com/cs/ww/de/view/109755475

WORKAROUNDS AND MITIGATIONS

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- Manually deactivate RCDP according to the instructions in the user guide. This measures completely mitigates the vulnerability.

GENERAL SECURITY RECOMMENDATIONS

As a general security measure, Siemens strongly recommends to protect network access to devices with appropriate mechanisms. In order to run the devices in a protected IT environment, Siemens particularly recommends to configure the environment according to Siemens' operational guidelines for Industrial Security (Download: https://www.siemens.com/cert/operational-guidelines-industrial-security), and to follow the recommendations in the product manuals.

Additional information on Industrial Security by Siemens can be found at: https://www.siemens.com/industrialsecurity

PRODUCT DESCRIPTION

RUGGEDCOM ROS-based devices, typically switches and serial-to-Ethernet devices, are used to connect devices that operate in harsh environments such as electric utility substations and traffic control cabinets.

SCALANCE X switches are used to connect industrial components like Programmable Logic Controllers (PLCs) or Human Machine Interfaces (HMIs).

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.0 (CVSS v3.0) (https://www.first.org/cvss/). The CVSS environmental score is specific to the customer's environment and will impact the overall CVSS score. The environmental score should therefore be individually defined by the customer to accomplish final scoring.

Vulnerability CVE-2017-12736

After initial configuration, the Ruggedcom Discovery Protocol (RCDP) is still able to writeto the device under certain conditions, potentially allowing users located in the adjacentnetwork of the targeted device to perform unauthorized administrative actions.

CVSS v3.0 Base Score	8.8
CVSS Vector	CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C

ADDITIONAL INFORMATION

For further inquiries on vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:

https://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2017-09-28):	Publication Date
V1.1 (2017-10-09):	Adjusted support team address for Ruggedcom devices
V1.2 (2018-02-22):	Added update information for SCALANCE XR-500/XM-400, and SCALANCE XB-200/XC-200/XP-200/XR300-WG

TERMS OF USE

Siemens Security Advisories are subject to the terms and conditions contained in Siemens’ underlying license terms or other applicable agreements previously agreed to with Siemens (hereinafter "License Terms"). To the extent applicable to information, software or documentation made available in or through a Siemens Security Advisory, the Terms of Use of Siemens’ Global Website (https://www.siemens.com/terms_of_use, hereinafter "Terms of Use"), in particular Sections 8-10 of the Terms of Use, shall apply additionally. In case of conflicts, the License Terms shall prevail over the Terms of Use.