SSA-363881: Web Vulnerabilities in RUGGEDCOM NMS

Publication Date 2017-02-22
Last Update 2017-02-22
Current Version V1.0
CVSS v3.0 Base Score 8.8

SUMMARY

The latest update for RUGGEDCOM NMS fixes two security vulnerabilities, which could allow a remote attacker to perform administrative operations under certain conditions.

AFFECTED PRODUCTS

- RUGGEDCOM NMS: All versions < V2.1 (Windows and Linux)

DESCRIPTION

RUGGEDCOM NMS is a scalable, fully-featured, enterprise-grade solution for monitoring, configuring and maintaining RUGGEDCOM mission-critical networks. It improves operational efficiency, speeds up system provisioning, and preserves data validity, while allowing focus on the key events in the network.

Detailed information about the vulnerabilities is provided below.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.0 (CVSS v3.0) (http://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 assessed by the customer to accomplish final scoring.

Vulnerability 1 (CVE-2017-2682)

The web application (port 8080/TCP and 8081/TCP) could allow a remote attacker to perform a Cross-Site Request Forgery (CSRF) attack, potentially allowing an attacker to execute administrative operations, provided the targeted user has an active session and is induced to trigger a malicious request.

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

Vulnerability 2 (CVE-2017-2683)

A non-privileged user of the web application (port 8080/TCP and 8081/TCP) could perform a persistent Cross-Site Scripting (XSS) attack, potentially resulting in obtaining administrative permissions.

CVSS Base Score 6.3
CVSS Vector CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:L/A:N/E:P/RL:O/RC:C

SOLUTION

Siemens provides RUGGEDCOM NMS V2.1 [1] which fixes the vulnerabilities and recommends customers to update to the new version.

As a general security measure Siemens strongly recommends to protect network access to the RUGGEDCOM NMS with appropriate mechanisms. It is advised to configure the environment according to our operational guidelines [2] in order to run the devices in a protected IT environment.

ADDITIONAL RESOURCES

[1] Information on how to obtain RUGGEDCOM NMS can be obtained here:
https://support.industry.siemens.com/cs/ww/en/view/109745179

[2] An overview of the operational guidelines for Industrial Security (with the cell protection concept):
https://www.siemens.com/cert/operational-guidelines-industrial-security

[3] Information about Industrial Security by Siemens:
https://www.siemens.com/industrialsecurity

[4] 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 (2017-02-22): Publication Date

DISCLAIMER