SSA-892342: Denial-of-Service Vulnerability in RuggedCom ROS-based Devices

Publication Date 2014-02-18
Last Update 2014-05-23
Current Version V1.3
CVSS Overall Score 2.0

Summary:

A potential vulnerability might allow attackers to perform a Denial-of-Service attack over the network without authentication on RuggedCom products running ROS.

Siemens address this issue by a firmware update [1].

AFFECTED PRODUCTS

All RuggedCom ROS-based devices running the following firmware version:

- All ROS versions before v3.11
- ROS v3.11 (for product RS950G): all versions < ROS v3.11.5
- ROS v3.12: all versions < ROS v3.12.4
- ROS v4.0 (for product RSG2488): all versions < ROS v4.1.0

DESCRIPTION

RuggedCom ROS-based products, 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.

A potential vulnerability in the implementation of the SNMP protocol might allow attackers to perform a Denial-of-Service attack on the affected devices over the network without authentication.

Detailed information about the vulnerability is provided below.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSSv2 scoring system (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 defined by the customer to accomplish final scoring.

Vulnerability Description (CVE-2014-1966)

The implementation of the SNMP protocol in the affected devices might allow attackers to perform a Denial-of-Service attack against the device's IP management interface by sending specially crafted packets over the network without authentication. Switching functionality is not affected and special and uncommon conditions must be fulfilled to perform this attack. After a manual cold restart of the device, access to the IP management interface is regained.

CVSS Base Score 2.6
CVSS Temporal Score 2.0
CVSS Overall Score 2.0 (AV:N/AC:H/Au:N/C:N/I:N/A:P/E:POC/RL:OF/RC:C)

Mitigating factors:

The attacker must have network access to the affected device. Special and uncommon conditions must be fulfilled to perform the attack.

SOLUTION

Siemens provide firmware updates ROS v3.11.5, ROS v3.12.4, and ROS v4.1.0 [1] which fix the vulnerability for RS950G products running ROS v3.11, products running ROS v3.12 and prior, and RSG2488 products running ROS v4.0.

As a general security measure Siemens strongly recommends to protect network access to the RuggedCom ROS-based devices with appropriate mechanisms. It is advised to follow recommended security practices [4] and to configure the environment according to operational guidelines [2] in order to run the devices in a protected IT environment.

ACKNOWLEDGEMENT

Siemens thanks the following for their support and efforts:

- Ling Toh Koh, Ng Yi Teng, Seyed Dawood Sajjadi Torshizi, Ryan Lee and Ho Ping Hou from EV-Dynamic, Malaysia for coordinated disclosure

ADDITIONAL RESOURCES

[1] The firmware updates for the RuggedCom ROS-based devices can be obtained for free from the following contact points:

- Submit a support request online: http://www.siemens.com/automation/support-request
- Call a local hotline center: http://www.automation.siemens.com/mcms/aspa-db/en/automation-technology/Pages/default.aspx

[2] An overview of the operational guidelines for Industrial Security (with the cell protection concept): http://www.industry.siemens.com/topics/global/en/industrial-security/Documents/operational_guidelines_industrial_security_en.pdf

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

[4] Recommended security practices by ICS-CERT: http://ics-cert.us-cert.gov/content/recommended-practices

[5] For further inquiries on vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT: http://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2014-02-18):	Publication Date
V1.1 (2014-03-11):	Rectified vulnerability description and CVSS score
V1.2 (2014-03-28):	Added solution for ROS v3.11, updated support contact points
V1.3 (2014-05-23):	Added solution for ROS v4.0

DISCLAIMER