SSA-831997: Denial-of-Service Vulnerability in Ruggedcom ROS-based Devices

Publication Date	2014-03-28
Last Update	2014-12-15
Current Version	V1.2
CVSS Overall Score	4.1

Summary:

A vulnerability might allow attackers to perform a Denial-of-Service attack over the network without prior authentication on the management web interface of Ruggedcom ROS-based devices.

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

AFFECTED PRODUCTS

The following Ruggedcom ROS-based products are affected:

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

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.

A vulnerability in the implementation of the web interface might allow attackers to perform a Denial-of-Service attack on the affected devices over the network without prior 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-2014-2590)

The implementation of the web server (port 80/tcp) in the affected devices might allow attackers to perform a Denial-of-Service attack against the device's management web interface by sending specially crafted packets over the network without prior authentication. It is not possible to exploit this attack via HTTPS (port 443/tcp), and switching functionality is not impacted. After a manual cold restart of the device, access to the web management interface is regained.

CVSS Base Score	5.0
CVSS Temporal Score	4.1
CVSS Overall Score	4.1 (AV:N/AC:L/Au:N/C:N/I:N/A:P/E:F/RL:OF/RC:C)

Mitigating Factors:

An attacker must have network access to the management interface of the affected devices. Siemens recommends operating the devices only within trusted networks [2].

SOLUTION

Siemens provides firmware updates [1] ROS v3.11.5 and ROS v4.1.1 which fix the vulnerability for RS950G products running ROS v3.11, RSG2488 products running ROS v4.0.0 and all other ROS based products running ROSv3.12.4 and below.

As a general security measure Siemens strongly recommends to protect network access to the management interface of Ruggedcom 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 Aivar Liimets from Martem Telecontrol Systems 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 (2014-03-28):	Publication Date
V1.1 (2014-05-23):	Added solution for all products except RSG2288, RS416 and RP110
V1.2 (2014-12-15):	Added ROS V4.1.1 which fixes the issue for RSG2288, RS416, and RP110

DISCLAIMER