SSA-324789: Vulnerabilities in RuggedCom ROS-based Devices

Publication Date	2013-12-06
Last Update	2013-12-06
Current Version	V1.0
CVSS Overall Score	6.5

Summary:

Multiple potential vulnerabilities, which might allow attackers to gain administrative access to the web interface over the network without authentication, were discovered in the web server authentication of all RuggedCom products running ROS.

These issues have been fixed in ROS firmware v3.12.2. RuggedCom and Siemens recommend upgrading to the current firmware version [1].

AFFECTED PRODUCTS

- RuggedCom devices with ROS version < ROS v3.12.2

DESCRIPTION

RuggedCom 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.

Potential vulnerabilities in the web server's authentication of the affected products might allow attackers to gain administrative access to the web interface over the network without authentication or unprivileged users to perform privilege escalation.

Detailed information about the vulnerabilities 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 1 (CVE-2013-6925)

The integrated web server (port 443/tcp) of the affected devices might allow attackers to guess the session id of an active web session and hijack it.

CVSS Base Score	8.3
CVSS Temporal Score	6.5
CVSS Overall Score	6.5 (AV:N/AC:M/Au:N/C:P/I:P/A:C/E:POC/RL:OF/RC:C)

Vulnerability 2 (CVE-2013-6926)

The integrated web server (port 443/tcp) of the affected devices might allow attackers with unprivileged accounts (guest or operator) to perform limited administrative operations over the network.

CVSS Base Score	8
CVSS Temporal Score	6.3
CVSS Overall Score	6.3 (AV:N/AC:L/Au:S/C:P/I:P/A:C/E:POC/RL:OF/RC:C)

Mitigating factors:

The attacker must have network access (port 443/tcp) to the affected devices for both vulnerabilities. For vulnerability 1, an administrator must use an active web session and the attacker must know the client IP address of the administrator. For vulnerability 2, credentials of an unprivileged account are needed.

SOLUTION

RuggedCom and Siemens recommend upgrading to the current firmware version ROS v.3.12.2 [1] which fixes the potential vulnerabilities.

As a general security measure Siemens strongly recommends to protect network access to the management interface of 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.

ADDITIONAL RESOURCES

[1] The firmware updates for the RuggedCom ROS-based devices can be obtained for free by contacting the RuggedCom support team at support@ruggedcom.com.

[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 (2013-12-06): Publication Date

DISCLAIMER

See: http://www.siemens.com/terms_of_use