SSA-396873: TLS Vulnerability in RUGGEDCOM ROS- and ROX-based Devices

Publication Date	2015-07-21
Last Update	2015-12-18
Current Version	V1.1
CVSS Overall Score	3.4

Summary:

The web interface of RUGGEDCOM ROS- and ROX-based devices is affected by a vulnerability that could allow remote attackers to recover parts of the plaintext of an encrypted connection under certain circumstances.

Siemens has released updates for ROS and ROX and recommends users to update to the latest firmware version.

AFFECTED PRODUCTS

- ROS: All Versions < 4.2.0
- ROX II: All Versions < 2.9.0

DESCRIPTION

RUGGEDCOM switches and ROX-based VPN endpoints and firewalls are used to connect devices that operate in harsh environments such as electric utility substations and traffic control cabinets.

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-2015-5537)

The web interface (TCP/port 443) of affected devices is vulnerable to a padding oracle attack (also known as TLS POODLE). A remote attacker in a privileged network position could possibly recover parts of the plain text if unsuspecting users are misled to click on a malicious link.

CVSS Base Score	4.3
CVSS Temporal Score	3.4
CVSS Overall Score	3.4 (AV:N/AC:M/Au:N/C:P/I:N/A:N/E:POC/RL:OF/RC:C)

Mitigating factors

An attacker must be in a position to perform a man-in-the-middle attack and mislead the user to click on a malicious link.

SOLUTION

Siemens provides firmware update v4.2.0 for ROS-based devices and firmware update v2.9.0 for ROX II-based devices which fix the vulnerability [1]. Siemens recommends users to update to the latest firmware versions.

Until patches can be applied, Siemens advises to apply the following steps to mitigate the risk:

- Disable the web interface on ROX II and use the SSH command line interface for configuration

or

- Restrict access to the web interface (TCP/port 443) to clients in trusted networks
- Do not access external sites while a web session to the web interface is active

As a general security measure Siemens strongly advises to follow security recommendations in the product manual [2, 3]. It is advised to configure the environment according to our operational guidelines [4] in order to run the devices in a protected IT environment.

ADDITIONAL RESOURCES

[1] The firmware updates for the affected products 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] Security recommendations for ROX-based devices are located in the manual: https://support.industry.siemens.com/cs/ww/en/ps/15320/man

[3] Security recommendations for ROS-based devices are located in the manual: https://support.industry.siemens.com/cs/ww/en/ps/15305/man

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

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

[6] 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 (2015-07-21): Publication Date
V1.1 (2015-12-18): Added update for ROX II

DISCLAIMER