SSA-921524: Incorrect Frame Padding in ROS-based Devices

Publication Date 2015-10-22
Last Update 2016-04-29
Current Version V1.1
CVSS Overall Score 2.7

Summary:

The latest firmware version for ROS-based devices fixes a vulnerability that could allow attackers to obtain parts of previous network traffic of other VLANs from Ethernet frame padding.

Siemens recommends users to update to the latest firmware version.

AFFECTED PRODUCTS

- ROS: All versions < V4.2.1
- ROS on the following products is not affected: RS950G

DESCRIPTION

RUGGEDCOM switches 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/v2). 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-2015-7836)

Affected devices do not pad Ethernet frames with null bytes, which could allow remote attackers in the adjacent network to obtain information of previous network packets from other VLANs.

CVSS Base Score 3.3
CVSS Temporal Score 2.7
CVSS Overall Score 2.7 (AV:A/AC:L/Au:N/C:P/I:N/A:N/E:F/RL:OF/RC:C)

SOLUTION

Siemens provides firmware update v4.2.1 for ROS-based devices [1] which fixes the vulnerability.

As a general security measure Siemens strongly advises to follow the security recommendations of the product manual [2]. Siemens also recommends the use of secure encrypted protocols like SSH or HTTPs. Additionally, it is advised to configure the environment according to our operational guidelines [3] in order to run the devices in a protected IT environment.

ACKNOWLEDGEMENT

Siemens thanks the following parties for their support and efforts:

- David Formby and Raheem Beyah of Georgia Tech for coordinated disclosure of the vulnerability.

- Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) for coordination efforts.

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 ROS-based devices are located in the manual: https://support.industry.siemens.com/cs/ww/en/ps/15305/man

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

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

[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 (2015-10-22): Publication Date
V1.1 (2016-04-29): Added information that ROS on RS950G is not affected

DISCLAIMER