SSA-839231: Incorrect Certificate Verification in Ruggedcom ROX-based Devices

Publication Date 2014-05-15
Last Update 2014-10-16
Current Version V1.2
CVSS Overall Score 4.5

Summary:

ROX-based Ruggedcom devices use GnuTLS libraries to enable secure communication. GnuTLS suffers from incorrect error handling in certificate verification which could allow Man-in-the-Middle (MITM) attacks, and this may affect multiple services in these devices.

Siemens has released firmware updates to mitigate the issue.

AFFECTED PRODUCTS

- ROX 1: V1.16.0
- ROX 2: V2.2 through V2.6 exclusive

DESCRIPTION

The following client-side services for Ruggedcom ROX-based devices use GnuTLS libraries and could allow MITM attacks:

- Secure Syslog (only affects ROX V1.16.0)
- Software upgrades with HTTPS-based connections. Non-secure connections are not affected. (Only affects ROX versions 2.4 and 2.5)
- FTPS (only affects ROX versions from 2.2 through 2.5 inclusive)

All other services are not affected. 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-2014-0092)

In Ruggedcom ROX-based devices, GnuTLS is used for client certificate verification. As GnuTLS is vulnerable to an incorrect error handling issue within this function, an attacker could be able to perform Man-in-the-Middle attacks.

CVSS Base Score 5.8
CVSS Temporal Score 4.5
CVSS Overall Score 4.5 (AV:N/AC:M/Au:N/C:P/I:P/A:N/E:POC/RL:OF/RC:C)

Mitigating factor:

The attacker must have network access to the affected devices and must be able to intercept and spoof network packets.

SOLUTION

Siemens provides firmware update V2.6.0 for ROX 2 [1] and firmware update V1.16.1 for ROX 1 [1] which fix the vulnerability.

It is advised to follow the recommended security practices [4] and to configure the environment according to the operational guidelines [2] in order to operate the devices in a protected IT environment.

ADDITIONAL RESOURCES

[1] The firmware updates for the Ruggedcom ROX-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 recommended 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 published by Siemens:
http://www.siemens.com/industrialsecurity

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

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

HISTORY DATA

V1.0 (2014-05-15): Publication date
V1.1 (2014-10-13): Added fix for ROX 2
V1.2 (2014-10-16): Added fix for ROX 1

DISCLAIMER