SSA-327980: Vulnerabilities in RUGGEDCOM ROX I

Publication Date 2017-03-28
Last Update 2017-03-28
Current Version V1.0
CVSS v3.0 Base Score 8.8

SUMMARY

RUGGEDCOM ROX I-based devices are affected by several vulnerabilities which could potentially allow attackers to perform actions with administrative privileges.

Siemens recommends specific countermeasures to mitigate the vulnerabilities in ROX I devices. Siemens will update this advisory when new information becomes available.

AFFECTED PRODUCTS

- RUGGEDCOM ROX I: All versions

DESCRIPTION

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

Detailed information about the vulnerabilities is provided below.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.0 (CVSS v3.0) (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 assessed by the customer to accomplish final scoring.

Vulnerability 1 (CVE-2017-2686)

An authenticated user could read arbitrary files through the web interface at port 10000/TCP and access sensitive information.

CVSS Base Score 6.5
CVSS Vector CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:T/RC:C

Vulnerability 2 (CVE-2017-2687)

The integrated web server at port 10000/TCP is prone to reflected Cross-Site Scripting attacks if an unsuspecting user is induced to click on a malicious link.

CVSS Base Score 6.1
CVSS Vector CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N/E:P/RL:T/RC:C

Vulnerability 3 (CVE-2017-2688)

The integrated web server at port 10000/TCP could allow remote attackers to perform actions with the privileges of an authenticated user, provided the targeted user has an active session and is induced into clicking on a malicious link or into visiting a malicious website.

CVSS Base Score 7.6
CVSS Vector CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:H/A:L/E:P/RL:T/RC:C

Vulnerability 4 (CVE-2017-2689)

An authenticated user could bypass access restrictions in the web interface at port 10000/TCP to obtain privileged file system access or change configuration settings.

CVSS Base Score 8.8
CVSS Vector CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:T/RC:C

Vulnerability 5 (CVE-2017-6864)

The integrated web server at port 10000/TCP could allow an authenticated user to perform stored Cross-Site Scripting attacks.

CVSS Base Score 6.4
CVSS Vector CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N/E:P/RL:T/RC:C

Mitigating Factors

The attacker must induce a user into clicking on a malicious link while a privileged session is open in the same browser in order to exploit vulnerability 2.

The attacker must induce a user into clicking on a malicious link or into visiting a malicious website while a privileged session is open in the same browser in order to exploit vulnerability 3.

The attacker must have network access to the web interface at port 10000/TCP of ROX I-based devices and possess valid credentials to exploit vulnerability 1, 4 and 5.

SOLUTION

Siemens recommends the following mitigations:

- Use the provided tool [1] and follow the application note [2] to:
  - Disable the web interface
  - Disable guest and operator accounts
- Restrict access to trusted administrators only
- Apply cell protection concept [3]
- Use VPN for protecting network communication between cells
- Apply Defense-in-Depth [3]

As a general security measure Siemens strongly recommends to protect network access to the web interface at 10000/TCP of ROX I-based devices with appropriate mechanisms. It is advised to configure the environment according to our operational guidelines [3] in order to run the devices in a protected IT environment.

ACKNOWLEDGEMENTS

Siemens thanks Maxim Rupp for coordinated disclosure of vulnerabilities 1-4.

ADDITIONAL RESOURCES

[1] The mitigation tool for the affected ROX I-based products can be obtained from the following contact points:
  - Submit a support request online
    https://www.siemens.com/automation/support-request
  - Call a local hotline center:
    https://w3.siemens.com/aspa_app/

[2] The ROX I mitigation tool supporting FAQ (application note) can be obtained from:
https://support.industry.siemens.com/cs/ww/en/view/109746106

[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:
https://www.siemens.com/industrialsecurity

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

HISTORY DATA

V1.0 (2017-03-28): Publication Date

DISCLAIMER