SSA-146325: Multiple Vulnerabilities in RUGGEDCOM ROX before V2.16

Publication Date: 2023-07-11
Last Update: 2023-07-11
Current Version: V1.0
CVSS v3.1 Base Score: 9.8

SUMMARY

Devices based on RUGGEDCOM ROX before V2.16 contain multiple high severity vulnerabilities, including the third-party vulnerabilities: CVE-2022-24903, CVE-2022-2068, CVE-2021-22946, CVE-2022-22576, CVE-2022-27781, CVE-2022-27782, CVE-2022-32207, CVE-2022-1292.

Siemens has released updates for the affected products and recommends to update to the latest versions.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
RUGGEDCOM ROX MX5000: All versions < V2.16.0	Update to V2.16.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109821187/
RUGGEDCOM ROX MX5000RE: All versions < V2.16.0	Update to V2.16.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109821187/
RUGGEDCOM ROX RX1400: All versions < V2.16.0	Update to V2.16.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109821187/
RUGGEDCOM ROX RX1500: All versions < V2.16.0	Update to V2.16.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109821187/
RUGGEDCOM ROX RX1501: All versions < V2.16.0	Update to V2.16.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109821187/
RUGGEDCOM ROX RX1510: All versions < V2.16.0	Update to V2.16.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109821187/
RUGGEDCOM ROX RX1511: All versions < V2.16.0	Update to V2.16.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109821187/
RUGGEDCOM ROX RX1512: All versions < V2.16.0	Update to V2.16.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109821187/

RUGGEDCOM ROX RX1524: All versions < V2.16.0	Update to V2.16.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109821187/
RUGGEDCOM ROX RX1536: All versions < V2.16.0	Update to V2.16.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109821187/
RUGGEDCOM ROX RX5000: All versions < V2.16.0	Update to V2.16.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109821187/

WORKAROUNDS AND MITIGATIONS

Product-specific remediations or mitigations can be found in the section Affected Products and Solution. Please follow the General Security Recommendations.

GENERAL SECURITY RECOMMENDATIONS

As a general security measure, Siemens strongly recommends to protect network access to devices with appropriate mechanisms. In order to operate the devices in a protected IT environment, Siemens recommends to configure the environment according to Siemens' operational guidelines for Industrial Security (Download: https://www.siemens.com/cert/operational-guidelines-industrial-security), and to follow the recommendations in the product manuals. Additional information on Industrial Security by Siemens can be found at: https://www.siemens.com/industrialsecurity

PRODUCT DESCRIPTION

RUGGEDCOM Ethernet switches are used to operate reliably in electrical harsh and climatically demanding environments such as electric utility substations and traffic control cabinets.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.1 (CVSS v3.1) (https://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.

An additional classification has been performed using the CWE classification, a community-developed list of common software security weaknesses. This serves as a common language and as a baseline for weakness identification, mitigation, and prevention efforts. A detailed list of CWE classes can be found at: https://cwe.mitre.org/.

Vulnerability CVE-2021-22946

A user can tell curl >= 7.20.0 and <= 7.78.0 to require a successful upgrade to TLS when speaking to an IMAP, POP3 or FTP server (`--ssl-reqd` on the command line or`CURLOPT_USE_SSL` set to `CURLUSESSL_CONTROL` or `CURLUSESSL_ALL` withlibcurl). This requirement could be bypassed if the server would return a properly crafted but perfectly legitimate response.This flaw would then make curl silently continue its operations **withoutTLS** contrary to the instructions and expectations, exposing possibly sensitive data in clear text over the network.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-319: Cleartext Transmission of Sensitive Information

Vulnerability CVE-2022-1292

The c_rehash script does not properly sanitise shell metacharacters to prevent command injection.

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

Vulnerability CVE-2022-2068

In addition to the c_rehash shell command injection identified in CVE-2022-1292, further circumstances where the c_rehash script does not properly sanitise shell metacharacters to prevent command injection were found by code review. When the CVE-2022-1292 was fixed it was not discovered that there are other places in the script where the file names of certificates being hashed were possibly passed to a command executed through the shell. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool.

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

Vulnerability CVE-2022-22576

An improper authentication vulnerability exists in curl 7.33.0 to and including 7.82.0 which might allow reuse OAUTH2-authenticated connections without properly making sure that the connection was authenticated with the same credentials as set for this transfer. This affects SASL-enabled protocols: SMPTP(S), IMAP(S), POP3(S) and LDAP(S) (openldap only).

CVSS v3.1 Base Score	8.1
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C
CWE	CWE-287: Improper Authentication

Vulnerability CVE-2022-24903

Rsyslog is a rocket-fast system for log processing. Modules for TCP syslog reception have a potential heap buffer overflow when octet-counted framing is used. This can result in a segfault or some other malfunction. As of our understanding, this vulnerability can not be used for remote code execution. But there may still be a slight chance for experts to do that. The bug occurs when the octet count is read. While there is a check for the maximum number of octets, digits are written to a heap buffer even when the octet count is over the maximum, This can be used to overrun the memory buffer. However, once the sequence of digits stop, no additional characters can be added to the buffer. In our opinion, this makes remote exploits impossible or at least highly complex. Octet-counted framing is one of two potential framing modes. It is relatively uncommon, but enabled by default on receivers. Modules `imtcp`, `imptcp`, `imgssapi`, and `imhttp` are used for regular syslog message reception. It is best practice not to directly expose them to the public. When this practice is followed, the risk is considerably lower. Module `imdiag` is a diagnostics module primarily intended for testbench runs. We do not expect it to be present on any production installation. Octet-counted framing is not very common. Usually, it needs to be specifically enabled at senders. If users do not need it, they can turn it off for the most important modules. This will mitigate the vulnerability.

CVSS v3.1 Base Score	8.1
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

Vulnerability CVE-2022-27781

libcurl provides the `CURLOPT_CERTINFO` option to allow applications torequest details to be returned about a server's certificate chain.Due to an erroneous function, a malicious server could make libcurl built withNSS get stuck in a never-ending busy-loop when trying to retrieve thatinformation.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-400: Uncontrolled Resource Consumption

Vulnerability CVE-2022-27782

libcurl would reuse a previously created connection even when a TLS or SSHrelated option had been changed that should have prohibited reuse.libcurl keeps previously used connections in a connection pool for subsequenttransfers to reuse if one of them matches the setup. However, several TLS andSSH settings were left out from the configuration match checks, making themmatch too easily.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C
CWE	CWE-295: Improper Certificate Validation

Vulnerability CVE-2022-29561

The web interface of the affected devices are vulnerable to Cross-Site Request Forgery attacks. By tricking an authenticated victim user to click a malicious link, an attacker could perform arbitrary actions on the device on behalf of the victim user.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-352: Cross-Site Request Forgery (CSRF)

Vulnerability CVE-2022-29562

Affected devices do not properly handle malformed HTTP packets. This could allow an unauthenticated remote attacker to send a malformed HTTP packet causing certain functions to fail in a controlled manner.

CVSS v3.1 Base Score	3.7
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2022-32207

When curl < 7.84.0 saves cookies, alt-svc and hsts data to local files, it makes the operation atomic by finalizing the operation with a rename from a temporary name to the final target file name.In that rename operation, it might accidentally *widen* the permissions for the target file, leaving the updated file accessible to more users than intended.

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-276: Incorrect Default Permissions

Vulnerability CVE-2023-36386

A reflected cross-site scripting (XSS) vulnerability exists in the web interface of the affected application that could allow an attacker to execute malicious javascript code by tricking users into accessing a malicious link. The value is reflected in the response without sanitization while throwing an “invalid params element name” error on the get_elements parameters.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-79: Improper Neutralization of Input During Web Page Generation (’Cross-site Scripting’)

Vulnerability CVE-2023-36389

A reflected cross-site scripting (XSS) vulnerability exists in the web interface of the affected application that could allow an attacker to execute malicious javascript code by tricking users into accessing a malicious link. The malformed value is reflected directly in the response without sanitization while throwing an “invalid path” error.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-79: Improper Neutralization of Input During Web Page Generation (’Cross-site Scripting’)

Vulnerability CVE-2023-36390

A reflected cross-site scripting (XSS) vulnerability exists in the web interface of the affected application that could allow an attacker to execute malicious javascript code by tricking users into accessing a malicious link. The value is reflected in the response without sanitization while throwing an “invalid params element name” error on the action parameters.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-79: Improper Neutralization of Input During Web Page Generation (’Cross-site Scripting’)

Vulnerability CVE-2023-36748

The affected devices are configured to offer weak ciphers by default. This could allow an unauthorized attacker in a man-in-the-middle position to read and modify any data passed over to and from the affected device.

CVSS v3.1 Base Score	5.9
CVSS Vector	CVSS:3.1/AV:A/AC:H/PR:N/UI:R/S:U/C:L/I:H/A:L/E:P/RL:O/RC:C
CWE	CWE-326: Inadequate Encryption Strength

Vulnerability CVE-2023-36749

The webserver of the affected devices support insecure TLS 1.0 protocol. An attacker could achieve a man-in-the-middle attack and compromise confidentiality and integrity of data.

CVSS v3.1 Base Score	7.4
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C
CWE	CWE-327: Use of a Broken or Risky Cryptographic Algorithm

Vulnerability CVE-2023-36750

The software-upgrade Url parameter in the web interface of affected devices is vulnerable to command injection due to missing server side input sanitation. This could allow an authenticated privileged remote attacker to execute arbitrary code with root privileges.

CVSS v3.1 Base Score	9.1
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection')

Vulnerability CVE-2023-36751

The install-app URL parameter in the web interface of affected devices is vulnerable to command injection due to missing server side input sanitation. This could allow an authenticated privileged remote attacker to execute arbitrary code with root privileges.

CVSS v3.1 Base Score	9.1
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection')

Vulnerability CVE-2023-36752

The upgrade-app URL parameter in the web interface of affected devices is vulnerable to command injection due to missing server side input sanitation. This could allow an authenticated privileged remote attacker to execute arbitrary code with root privileges.

CVSS v3.1 Base Score	9.1
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection')

Vulnerability CVE-2023-36753

The uninstall-app App-name parameter in the web interface of affected devices is vulnerable to command injection due to missing server side input sanitation. This could allow an authenticated privileged remote attacker to execute arbitrary code with root privileges.

CVSS v3.1 Base Score	9.1
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection')

Vulnerability CVE-2023-36754

The SCEP server configuration URL parameter in the web interface of affected devices is vulnerable to command injection due to missing server side input sanitation. This could allow an authenticated privileged remote attacker to execute arbitrary code with root privileges.

CVSS v3.1 Base Score	9.1
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection')

Vulnerability CVE-2023-36755

The SCEP CA Certificate Name parameter in the web interface of affected devices is vulnerable to command injection due to missing server side input sanitation. This could allow an authenticated privileged remote attacker to execute arbitrary code with root privileges.

CVSS v3.1 Base Score	9.1
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection')

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- James Clee for reporting the vulnerabilities CVE-2022-29561, CVE-2023-36750, CVE-2023-36751, CVE-2023-36752, CVE-2023-36753, CVE-2023-36754 and CVE-2023-36755
- Michael Messner from Siemens Energy for reporting the vulnerabilities CVE-2023-36386, CVE-2023-36389 and CVE-2023-36390

ADDITIONAL INFORMATION

For further inquiries on security vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:

https://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2023-07-11): Publication Date

TERMS OF USE