SSA-732250: Libcurl Vulnerabilities in Industrial Devices

Publication Date: 2022-05-10
Last Update: 2022-05-10
Current Version: V1.0
CVSS v3.1 Base Score: 8.1

SUMMARY

Vulnerabilities in third-party component cURL could allow an attacker to interfere with the affected products in various ways.

Siemens has released updates for several affected products and recommends to update to the latest versions. Siemens is preparing further updates and recommends countermeasures for products where updates are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
LOGO! CMR family: All versions only affected by CVE-2021-22924	Currently no fix is available • For CVE-2021-22924: Use the certificate projection feature to pin the valid certificates of external servers providing the services E-mail and DynDNS to the affected devices. To do this, see the description in the sections “Ca Certificate” in the chapters “E-Mail” and “DynDNS” in the manual
RUGGEDCOM RM1224 LTE(4G) EU (6GK6108-4AM00-2BA2): All versions < V7.1 only affected by CVE-2021-22924	Update to V7.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109807276
RUGGEDCOM RM1224 LTE(4G) NAM (6GK6108-4AM00-2DA2): All versions < V7.1 only affected by CVE-2021-22924	Update to V7.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109807276
SCALANCE M804PB (6GK5804-0AP00-2AA2): All versions < V7.1 only affected by CVE-2021-22924	Update to V7.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109807276
SCALANCE M812-1 ADSL-Router (Annex A) (6GK5812-1AA00-2AA2): All versions < V7.1 only affected by CVE-2021-22924	Update to V7.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109807276
SCALANCE M812-1 ADSL-Router (Annex B) (6GK5812-1BA00-2AA2): All versions < V7.1 only affected by CVE-2021-22924	Update to V7.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109807276

SCALANCE M816-1 ADSL-Router (Annex A) (6GK5816-1AA00-2AA2): All versions < V7.1 only affected by CVE-2021-22924	Update to V7.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109807276
SCALANCE M816-1 ADSL-Router (Annex B) (6GK5816-1BA00-2AA2): All versions < V7.1 only affected by CVE-2021-22924	Update to V7.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109807276
SCALANCE M826-2 SHDSL-Router (6GK5826-2AB00-2AB2): All versions < V7.1 only affected by CVE-2021-22924	Update to V7.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109807276
SCALANCE M874-2 (6GK5874-2AA00-2AA2): All versions < V7.1 only affected by CVE-2021-22924	Update to V7.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109807276
SCALANCE M874-3 (6GK5874-3AA00-2AA2): All versions < V7.1 only affected by CVE-2021-22924	Update to V7.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109807276
SCALANCE M876-3 (EVDO) (6GK5876-3AA02-2BA2): All versions < V7.1 only affected by CVE-2021-22924	Update to V7.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109807276
SCALANCE M876-3 (ROK) (6GK5876-3AA02-2EA2): All versions < V7.1 only affected by CVE-2021-22924	Update to V7.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109807276
SCALANCE M876-4 (EU) (6GK5876-4AA00-2BA2): All versions < V7.1 only affected by CVE-2021-22924	Update to V7.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109807276
SCALANCE M876-4 (NAM) (6GK5876-4AA00-2DA2): All versions < V7.1 only affected by CVE-2021-22924	Update to V7.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109807276
SCALANCE MUM856-1 (EU) (6GK5856-2EA00-3DA1): All versions < V7.1 only affected by CVE-2021-22924	Update to V7.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109807276
SCALANCE MUM856-1 (RoW) (6GK5856-2EA00-3AA1): All versions < V7.1 only affected by CVE-2021-22924	Update to V7.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109807276

SCALANCE S615 (6GK5615-0AA00-2AA2): All versions < V7.1 only affected by CVE-2021-22924	Update to V7.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109807276
SIMATIC CP 1543-1 (6GK7543-1AX00-0XE0): All versions < V3.0.22	Update to V3.0.22 or later version https://support.industry.siemens.com/cs/ww/en/view/109808678
SIMATIC CP 1545-1 (6GK7545-1GX00-0XE0): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SIMATIC RTU3010C (6NH3112-0BA00-0XX0): All versions < V5.0.14 only affected by CVE-2021-22924	Update to V5.0.14 or later version https://support.industry.siemens.com/cs/ww/en/view/109810215/
SIMATIC RTU3030C (6NH3112-3BA00-0XX0): All versions < V5.0.14 only affected by CVE-2021-22924	Update to V5.0.14 or later version https://support.industry.siemens.com/cs/ww/en/view/109810215/
SIMATIC RTU3031C (6NH3112-3BB00-0XX0): All versions < V5.0.14 only affected by CVE-2021-22924	Update to V5.0.14 or later version https://support.industry.siemens.com/cs/ww/en/view/109810215/
SIMATIC RTU3041C (6NH3112-4BB00-0XX0): All versions < V5.0.14 only affected by CVE-2021-22924	Update to V5.0.14 or later version https://support.industry.siemens.com/cs/ww/en/view/109810215/
SIPLUS NET CP 1543-1 (6AG1543-1AX00-2XE0): All versions < V3.0.22	Update to V3.0.22 or later version https://support.industry.siemens.com/cs/ww/en/view/109808678

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

The devices of the LOGO! CMR family (in combination with the LOGO! logic module) are cost-efficient communication systems suitable for monitoring and controlling distributed plants and systems via text message or email. LOGO! CMR devices can send text messages or emails to predefined mobile network numbers as well as receive text messages from predefined mobile network numbers. The LOGO! CMR devices offer comfortable Web Based Management commissioning and diagnostics via local and/or remote access.

The devices of the RTU3000C family are compact telecontrol stations for applications with their own power supply for autonomous energy systems. They are particularly suited for monitoring and control of external stations that are not connected to an energy supply network. The RTUs can autonomously record data with time stamp from connected sensors, pre-process this data and transfer it to a control center.

The SCALANCE M-800, MUM-800 and S615 as well as the RUGGEDCOM RM1224 industrial routers are used for secure remote access to plants via mobile networks, e.g. GPRS or UMTS with the integrated security functions of a firewall for protection against unauthorized access and VPN to protect data transmission.

The SIMATIC CP 1543-1 communication processor connects the S7-1500 controller to Ethernet networks. It provides integrated security functions such as firewall, Virtual Private Networks (VPN) and support of other protocols with data encryption such as FTPs. The communication processor protects S7-1500 stations against unauthorized access, as well as integrity and confidentiality of transmitted data.

The SIMATIC CP 1545-1 communication processor connects the S7-1500 controller to Ethernet networks. It provides integrated security functions such as firewall, Virtual Private Networks (VPN) and support of other protocols with data encryption. The communication processor protects S7-1500 stations against unauthorized access, as well as integrity and confidentiality of transmitted data.

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-2021-22901

curl 7.75.0 through 7.76.1 suffers from a use-after-free vulnerability resulting in already freed memory being used when a TLS 1.3 session ticket arrives over a connection. A malicious server can use this in rare unfortunate circumstances to potentially reach remote code execution in the client. When libcurl at run-time sets up support for TLS 1.3 session tickets on a connection using OpenSSL, it stores pointers to the transfer in-memory object for later retrieval when a session ticket arrives. If the connection is used by multiple transfers (like with a reused HTTP/1.1 connection or multiplexed HTTP/2 connection) that first transfer object might be freed before the new session is established on that connection and then the function will access a memory buffer that might be freed. When using that memory, libcurl might even call a function pointer in the object, making it possible for a remote code execution if the server could somehow manage to get crafted memory content into the correct place in memory.

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-416: Use After Free

Vulnerability CVE-2021-22924

libcurl keeps previously used connections in a connection pool for subsequent transfers to reuse, if one of them matches the setup. Due to errors in the logic, the config matching function did not take ‘issuercert’ into account and it compared the involved paths *case insensitively*,which could lead to libcurl reusing wrong connections. File paths are, or can be, case sensitive on many systems but not all, and can even vary depending on used file systems. The comparison also didn’t include the ‘issuer cert’ which a transfer can set to qualify how to verify the server certificate.

CVSS v3.1 Base Score	3.7
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-706: Use of Incorrectly-Resolved Name or Reference

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 (2022-05-10): Publication Date

TERMS OF USE

Siemens Security Advisories are subject to the terms and conditions contained in Siemens’ underlying license terms or other applicable agreements previously agreed to with Siemens (hereinafter "License Terms"). To the extent applicable to information, software or documentation made available in or through a Siemens Security Advisory, the Terms of Use of Siemens’ Global Website (https://www.siemens.com/terms_of_use, hereinafter "Terms of Use"), in particular Sections 8-10 of the Terms of Use, shall apply additionally. In case of conflicts, the License Terms shall prevail over the Terms of Use.