SSA-333517: Multiple Vulnerabilities in SCALANCE SC-600 Family before V3.0

Publication Date: 2022-12-13
Last Update: 2022-12-13
Current Version: V1.0
CVSS v3.1 Base Score: 7.8

SUMMARY

Multiple vulnerabilities affecting various third-party components of the SCALANCE SC-600 family could allow an attacker to cause a denial of service condition, corrupt memory or potentially execute custom code.

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
SCALANCE SC622-2C (6GK5622-2GS00-2AC2): All versions < V3.0	Update to V3.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109814276/
SCALANCE SC626-2C (6GK5626-2GS00-2AC2): All versions < V3.0	Update to V3.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109814276/
SCALANCE SC632-2C (6GK5632-2GS00-2AC2): All versions < V3.0	Update to V3.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109814276/
SCALANCE SC636-2C (6GK5636-2GS00-2AC2): All versions < V3.0	Update to V3.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109814276/
SCALANCE SC642-2C (6GK5642-2GS00-2AC2): All versions < V3.0	Update to V3.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109814276/
SCALANCE SC646-2C (6GK5646-2GS00-2AC2): All versions < V3.0	Update to V3.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109814276/

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

SCALANCE SC-600 devices (SC622-2C, SC626-2C, SC632-2C, SC636-2C, SC642-2C, SC646-2C) are used to protect trusted industrial networks from untrusted networks. They allow filtering incoming and outgoing network connections in different ways.

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-2018-25032

zlib before 1.2.12 allows memory corruption when deflating (i.e., when compressing) if the input has many distant matches.

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-787: Out-of-bounds Write

Vulnerability CVE-2022-30065

A use-after-free in Busybox 1.35-x's awk applet leads to denial of service and possibly code execution when processing a crafted awk pattern in the copyvar function.

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-416: Use After Free

Vulnerability CVE-2022-32205

A malicious server can serve excessive amounts of “Set-Cookie:” headers in a HTTP response to curl and curl < 7.84.0 stores all of them. A sufficiently large amount of (big) cookies make subsequent HTTP requests to this, or other servers to which the cookies match, create requests that become larger than the threshold that curl uses internally to avoid sending crazy large requests (1048576 bytes) and instead returns an error.This denial state might remain for as long as the same cookies are kept, match and haven’t expired. Due to cookie matching rules, a server on “foo.example.com” can set cookies that also would match for “bar.example.com”, making it it possible for a “sister server” to effectively cause a denial of service for a sibling site on the same second level domain using this method.

CVSS v3.1 Base Score	4.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C
CWE	CWE-770: Allocation of Resources Without Limits or Throttling

Vulnerability CVE-2022-32206

curl < 7.84.0 supports “chained” HTTP compression algorithms, meaning that a serverresponse can be compressed multiple times and potentially with different algorithms. The number of acceptable “links” in this “decompression chain” was unbounded, allowing a malicious server to insert a virtually unlimited number of compression steps.The use of such a decompression chain could result in a “malloc bomb”, makingcurl end up spending enormous amounts of allocated heap memory, or trying toand returning out of memory errors.

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-770: Allocation of Resources Without Limits or Throttling

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 (2022-12-13): 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.