

SSA-558014: Third-Party Component Vulnerabilities in SCALANCE XCM332 before V2.2

Publication Date: 2023-04-11
Last Update: 2023-04-11
Current Version: V1.0
CVSS v3.1 Base Score: 9.8

SUMMARY

Multiple vulnerabilities in the third-party components cURL, BusyBox, libtirpc, Expat as well as in the Linux Kernel could allow an attacker to impact the SCALANCE XCM332 device's confidentiality, integrity and availability.

Siemens has released an update for the SCALANCE XCM332 and recommends to update to the latest version.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SCALANCE XCM332 (6GK5332-0GA01-2AC2): All versions < V2.2	Update to V2.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109817513/

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 X switches are used to connect industrial components like Programmable Logic Controllers (PLCs) or Human Machine Interfaces (HMIs).

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-2021-46828

In libtirpc before 1.3.3rc1, remote attackers could exhaust the file descriptors of a process that uses libtirpc because idle TCP connections are mishandled. This can, in turn, lead to an svc_run infinite loop without accepting new connections.

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
CWE	CWE-770: Allocation of Resources Without Limits or Throttling

Vulnerability CVE-2022-1652

Linux Kernel could allow a local attacker to execute arbitrary code on the system, caused by a concurrency use-after-free flaw in the bad_flp_intr function. By executing a specially-crafted program, an attacker could exploit this vulnerability to execute arbitrary code or cause a denial of service condition on the system.

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

Vulnerability CVE-2022-1729

A race condition was found the Linux kernel in perf_event_open() which can be exploited by an unprivileged user to gain root privileges. The bug allows to build several exploit primitives such as kernel address information leak, arbitrary execution, etc.

CVSS v3.1 Base Score	7.0
CVSS Vector	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')

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 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 server response 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", making curl end up spending enormous amounts of allocated heap memory, or trying to and 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

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-2022-32208

When curl < 7.84.0 does FTP transfers secured by krb5, it handles message verification failures wrongly. This flaw makes it possible for a Man-In-The-Middle attack to go unnoticed and even allows it to inject data to the client.

CVSS v3.1 Base Score 5.9
CVSS Vector [CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C](#)
CWE CWE-787: Out-of-bounds Write

Vulnerability CVE-2022-35252

When curl is used to retrieve and parse cookies from a HTTP(S) server, it accepts cookies using control codes that when later are sent back to a HTTP server might make the server return 400 responses. Effectively allowing a "sister site" to deny service to all siblings.

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:U/RL:O/RC:C](#)
CWE CWE-1286: Improper Validation of Syntactic Correctness of Input

Vulnerability CVE-2022-40674

libexpat before 2.4.9 has a use-after-free in the doContent function in xmlparse.c.

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-416: Use After Free

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 (2023-04-11): 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.