SSA-942865: Multiple Vulnerabilities in the Integrated SCALANCE S615 of SINAMICS Medium Voltage Products

Publication Date: 2023-06-13
Last Update: 2023-06-14
Current Version: V1.1
CVSS v3.1 Base Score: 9.8

SUMMARY

SINAMICS PERFECT HARMONY GH180 is affected by multiple vulnerabilities in the integrated SCALANCE S615 device, as documented in SSA-419740 (https://cert-portal.siemens.com/productcert/html/ssa-419740.html).

Siemens recommends to update the firmware of the integrated SCALANCE S615 device to the latest version. Siemens recommends specific countermeasures for products where the firmware update is not, or not yet applied.

Additional considerations regarding the specific impact of the vulnerabilities to SINAMICS MV products can be found in the chapter “Additional Information”.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SINAMICS PERFECT HARMONY GH180 6SR5: All versions only when produced between Oct 2021 and May 2023 and with installed SCALANCE S615 device	Update the firmware of the integrated SCALANCE S615 device to V7.2 or later version See further recommendations from section Workarounds and Mitigations

WORKAROUNDS AND MITIGATIONS

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- Restrict physical access to the affected drives, also to their Ethernet Port included on the front of the control door
- Disconnect any direct network connection to the integrated SCALANCE S615 device

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

SINAMICS medium voltage drives are used to control a wide variety of medium voltage converters or inverters in different applications.

The SINAMICS PERFECT HARMONY GH180 medium voltage drive family is used to control a wide variety of medium voltage converters or inverters in different applications.

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-2021-42374

An out-of-bounds heap read in Busybox's unlzma applet leads to information leak and denial of service when crafted LZMA-compressed input is decompressed. This can be triggered by any applet/format that internally supports LZMA compression.

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2021-42378

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

CVSS v3.1 Base Score	6.6
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-416: Use After Free

Vulnerability CVE-2021-42379

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

CVSS v3.1 Base Score	6.6
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-416: Use After Free

Vulnerability CVE-2021-42380

A use-after-free in awk leads to denial of service and possibly code execution when processing a crafted awk pattern in the clrvar function.

CVSS v3.1 Base Score	6.6
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-416: Use After Free

Vulnerability CVE-2021-42381

A use-after-free in awk leads to denial of service and possibly code execution when processing a crafted awk pattern in the hash_init function.

CVSS v3.1 Base Score	6.6
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-416: Use After Free

Vulnerability CVE-2021-42382

A use-after-free in awk leads to denial of service and possibly code execution when processing a crafted awk pattern in the getvar_s function.

CVSS v3.1 Base Score	6.6
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-416: Use After Free

Vulnerability CVE-2021-42383

A use-after-free in awk leads to denial of service and possibly code execution when processing a crafted awk pattern in the evaluate function.

CVSS v3.1 Base Score	6.6
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-416: Use After Free

Vulnerability CVE-2021-42384

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

CVSS v3.1 Base Score	6.6
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-416: Use After Free

Vulnerability CVE-2021-42385

A use-after-free in awk leads to denial of service and possibly code execution when processing a crafted awk pattern in the evaluate function.

CVSS v3.1 Base Score	6.6
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-416: Use After Free

Vulnerability CVE-2021-42386

A use-after-free in awk leads to denial of service and possibly code execution when processing a crafted awk pattern in the nvalloc function.

CVSS v3.1 Base Score	6.6
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-416: Use After Free

Vulnerability CVE-2022-0547

OpenVPN 2.1 until v2.4.12 and v2.5.6 may enable authentication bypass in external authentication plug-ins when more than one of them makes use of deferred authentication replies, which allows an external user to be granted access with only partially correct credentials.

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-287: Improper Authentication

Vulnerability CVE-2022-1199

A flaw was found in the Linux kernel. This flaw allows an attacker to crash the Linux kernel by simulating amateur radio from the user space, resulting in a null-ptr-deref vulnerability and a use-after-free vulnerability.

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-416: Use After Free

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-2022-1343

Under certain circumstances, the command line OCSP verify function reports successful verification when the verification in fact failed. In this case the incorrect successful response will also be accompanied by error messages showing the failure and contradicting the apparently successful result.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C
CWE	CWE-295: Improper Certificate Validation

Vulnerability CVE-2022-1473

The used OpenSSL version improperly reuses memory when decoding certificates or keys. This can lead to a process termination and Denial of Service for long lived processes.

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-404: Improper Resource Shutdown or Release

Vulnerability CVE-2022-23308

valid.c in libxml2 before 2.9.13 has a use-after-free of ID and IDREF attributes.

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-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

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, itaccepts cookies using control codes that when later are sent back to a HTTPserver 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-2022-36946

nfqnl_mangle in net/netfilter/nfnetlink_queue.c in the Linux kernel through 5.18.14 allows remote attackers to cause a denial of service (panic) because, in the case of an nf_queue verdict with a one-byte nfta_payload attribute, an skb_pull can encounter a negative skb->len.

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-20: Improper Input Validation

ADDITIONAL INFORMATION

Fieldbus network connections of the listed products (Modbus RTU, Modbus TCP, Profibus, ProfiNet, EtherNet/IP, DeviceNet, and ControlNet) are unaffected by the vulnerabilities.

The availability impact of the vulnerabilities is limited to the SCALANCE S615 device. While a successful exploitation could disrupt remote connections (e.g., SIDriveIQ remote monitoring), the normal functionality of the product itself is unaffected.
Consequently, in the context of the products listed in this advisory the CVSS vectors change as follows:

- Availability Impact (A): if A:H is set, change to A:L

For more information regarding the vulnerabilities in SCALANCE S615 devices refer to the Siemens Security Advisory SSA-419740 (https://cert-portal.siemens.com/productcert/html/ssa-419740.html).

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 (2023-06-13):	Publication Date
V1.1 (2023-06-14):	Removed not affected products SINAMICS GL150 and SINAMICS SL150

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.