SSA-892048: Third-Party Component Vulnerabilities in SINEC NMS before V1.0.3.1

Publication Date:	2023-05-09
Last Update:	2023-05-09
Current Version:	V1.0
CVSS v3.1 Base Score:	9.8

SUMMARY

Multiple vulnerabilities affecting third-party components libexpat and libcurl of SINEC NMS before V1.0.3.1 could allow an attacker to impact SINEC NMS confidentiality, integrity and availability.

Siemens has released an update for SINEC NMS and recommends to update to the latest version.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SINEC NMS: All versions < V1.0.3.1	Update to V1.0.3.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109818269/

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

SINEC NMS is a new generation of the Network Management System (NMS) for the Digital Enterprise. This system can be used to centrally monitor, manage, and configure networks.

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-2022-32221

When doing HTTP(S) transfers, libcurl might erroneously use the read callback (CURLOPT_READFUNCTION) to ask for data to send, even when the CURLOPT_POSTFIELDS option has been set, if the same handle previously was used to issue a PUT request which used that callback. This flaw may surprise the application and cause it to misbehave and either send off the wrong data or use memory after free or similar in the subsequent POST request. The problem exists in the logic for a reused handle when it is changed from a PUT to a POST.

CVSS v3.1 Base Score	8.2
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N/E:P/RL:O/RC:C
CWE	CWE-440: Expected Behavior Violation

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-2022-35260

curl can be told to parse a .netrc file for credentials. If that file endsin a line with 4095 consecutive non-white space letters and no newline, curlwould first read past the end of the stack-based buffer, and if the readworks, write a zero byte beyond its boundary.This will in most cases cause a segfault or similar, but circumstances might also cause different outcomes.If a malicious user can provide a custom netrc file to an application or otherwise affect its contents, this flaw could be used as denial-of-service.

CVSS v3.1 Base Score	8.6
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H/E:U/RL:O/RC:C
CWE	CWE-121: Stack-based Buffer Overflow

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

Vulnerability CVE-2022-42915

curl before 7.86.0 has a double free. If curl is told to use an HTTP proxy for a transfer with a non-HTTP(S) URL, it sets up the connection to the remote server by issuing a CONNECT request to the proxy, and then tunnels the rest of the protocol through. An HTTP proxy might refuse this request (HTTP proxies often only allow outgoing connections to specific port numbers, like 443 for HTTPS) and instead return a non-200 status code to the client. Due to flaws in the error/cleanup handling, this could trigger a double free in curl if one of the following schemes were used in the URL for the transfer: dict, gopher, gophers, ldap, ldaps, rtmp, rtmps, or telnet. The earliest affected version is 7.77.0.

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-415: Double Free

Vulnerability CVE-2022-42916

In curl before 7.86.0, the HSTS check could be bypassed to trick it into staying with HTTP. Using its HSTS support, curl can be instructed to use HTTPS directly (instead of using an insecure cleartext HTTP step) even when HTTP is provided in the URL. This mechanism could be bypassed if the host name in the given URL uses IDN characters that get replaced with ASCII counterparts as part of the IDN conversion, e.g., using the character UTF-8 U+3002 (IDEOGRAPHIC FULL STOP) instead of the common ASCII full stop of U+002E (.). The earliest affected version is 7.77.0 2021-05-26.

CVSS v3.1 Base Score	9.1
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N/E:U/RL:O/RC:C
CWE	CWE-319: Cleartext Transmission of Sensitive Information

Vulnerability CVE-2022-43551

A vulnerability exists in curl <7.87.0 HSTS check that could be bypassed to trick it to keep using HTTP. Using its HSTS support, curl can be instructed to use HTTPS instead of using an insecure clear-text HTTP step even when HTTP is provided in the URL. However, the HSTS mechanism could be bypassed if the host name in the given URL first uses IDN characters that get replaced to ASCII counterparts as part of the IDN conversion. Like using the character UTF-8 U+3002 (IDEOGRAPHIC FULL STOP) instead of the common ASCII full stop (U+002E) .. Then in a subsequent request, it does not detect the HSTS state and makes a clear text transfer. Because it would store the info IDN encoded but look for it IDN decoded.

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-2022-43552

curl can be asked to tunnel virtually all protocols it supports through an HTTP proxy. HTTP proxies can (and often do) deny such tunnel operations using an appropriate HTTP error response code. When getting denied to tunnel the specific protocols SMB or TELNET, curl would use a heap-allocated struct after it had been freed, in its transfer shutdown code path.

CVSS v3.1 Base Score	5.9
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C
CWE	CWE-416: Use After Free

Vulnerability CVE-2022-43680

In libexpat through 2.4.9, there is a use-after free caused by overeager destruction of a shared DTD in XML_ExternalEntityParserCreate in out-of-memory situations.

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

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 (2023-05-09):	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.