SSA-484086: Multiple Vulnerabilities in SINEMA Remote Connect Server before V3.1

Publication Date: 2022-06-14
Last Update: 2024-07-09
Current Version: V1.1
CVSS v3.1 Base Score: 9.8

SUMMARY

SINEMA Remote Connect Server is affected by multiple vulnerabilities, including

- A cross-site scripting vulnerability in an error message pop up window (CVE-2022-29034)
- Several authentication bypass, privilege escalation and integrity check vulnerabilities (CVE-2022-32251 through -32261)
- A command injection vulnerability in the file upload service (CVE-2022-32262)
- A chosen-plaintext attack against HTTP over TLS ("BREACH", CVE-2022-27221)
- Information disclosure vulnerabilities in the curl component (CVE-2021-22924 through -22925)
- Several vulnerabilities in the libexpat library, that could be exploited when the server is parsing untrusted XML files (CVE-2021-45960, CVE-2021-46143, CVE-2022-22822 through -22827, CVE-2022-23852, CVE-2022-23990, CVE-2022-25235 through -25236, CVE-2022-25313 through -25315.

Siemens has released an update for the SINEMA Remote Connect Server and recommends to update to the latest version. Note that the update also contains additional fixes for vulnerabilities documented in Siemens Security Advisories SSA-244969, SSA-539476, SSA-685781 and SSA-712929.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SINEMA Remote Connect Server: All versions < V3.1 affected by all CVEs	Update to V3.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109811169/

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

SINEMA Remote Connect is a management platform for remote networks that enables the simple management of tunnel connections (VPN) between headquarters, service technicians, and installed machines or plants. It provides both the Remote Connect Server, which is the server application, and the Remote Connect Client, which is an OpenVPN client for optimal connection to SINEMA Remote Connect Server.

VULNERABILITY DESCRIPTION

This chapter describes all vulnerabilities (CVE-IDs) addressed in this security advisory. Wherever applicable, it also documents the product-specific impact of the individual vulnerabilities.

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

Vulnerability CVE-2021-22925

curl supports the `-t` command line option, known as `CURLOPT_TELNETOPTIONS` in libcurl. This rarely used option is used to send variable=content pairs to TELNET servers. Due to flaw in the option parser for sending `NEW_ENV` variables, libcurl could be made to pass on uninitialized data from a stack based buffer to the server. Therefore potentially revealing sensitive internal information to the server using a clear-text network protocol. This could happen because curl did not call and use sscanf() correctly when parsing the string provided by the application.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-908: Use of Uninitialized Resource

Vulnerability CVE-2021-45960

In Expat (aka libexpat) before 2.4.3, a left shift by 29 (or more) places in the storeAtts function in xmlparse.c can lead to realloc misbehavior (e.g., allocating too few bytes, or only freeing memory).

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-400: Uncontrolled Resource Consumption

Vulnerability CVE-2021-46143

In doProlog in xmlparse.c in Expat (aka libexpat) before 2.4.3, an integer overflow exists for m_groupSize.

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-190: Integer Overflow or Wraparound

Vulnerability CVE-2022-22822

addBinding in xmlparse.c in Expat (aka libexpat) before 2.4.3 has an integer overflow.

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-190: Integer Overflow or Wraparound

Vulnerability CVE-2022-22823

build_model in xmlparse.c in Expat (aka libexpat) before 2.4.3 has an integer overflow.

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-190: Integer Overflow or Wraparound

Vulnerability CVE-2022-22824

defineAttribute in xmlparse.c in Expat (aka libexpat) before 2.4.3 has an integer overflow.

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-190: Integer Overflow or Wraparound

Vulnerability CVE-2022-22825

lookup in xmlparse.c in Expat (aka libexpat) before 2.4.3 has an integer overflow.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-190: Integer Overflow or Wraparound

Vulnerability CVE-2022-22826

nextScaffoldPart in xmlparse.c in Expat (aka libexpat) before 2.4.3 has an integer overflow.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-190: Integer Overflow or Wraparound

Vulnerability CVE-2022-22827

storeAtts in xmlparse.c in Expat (aka libexpat) before 2.4.3 has an integer overflow.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-190: Integer Overflow or Wraparound

Vulnerability CVE-2022-23852

Expat (aka libexpat) before 2.4.4 has a signed integer overflow in XML_GetBuffer, for configurations with a nonzero XML_CONTEXT_BYTES.

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-190: Integer Overflow or Wraparound

Vulnerability CVE-2022-23990

Expat (aka libexpat) before 2.4.4 has an integer overflow in the doProlog function.

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-190: Integer Overflow or Wraparound

Vulnerability CVE-2022-25235

xmltok_impl.c in Expat (aka libexpat) before 2.4.5 lacks certain validation of encoding, such as checks for whether a UTF-8 character is valid in a certain context.

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-116: Improper Encoding or Escaping of Output

Vulnerability CVE-2022-25236

xmlparse.c in Expat (aka libexpat) before 2.4.5 allows attackers to insert namespace-separator characters into namespace URIs.

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-668: Exposure of Resource to Wrong Sphere

Vulnerability CVE-2022-25313

In Expat (aka libexpat) before 2.4.5, an attacker can trigger stack exhaustion in build_model via a large nesting depth in the DTD element.

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-400: Uncontrolled Resource Consumption

Vulnerability CVE-2022-25314

In Expat (aka libexpat) before 2.4.5, there is an integer overflow in copyString.

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-190: Integer Overflow or Wraparound

Vulnerability CVE-2022-25315

In Expat (aka libexpat) before 2.4.5, there is an integer overflow in storeRawNames.

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-190: Integer Overflow or Wraparound

Vulnerability CVE-2022-27221

An attacker in machine-in-the-middle could obtain plaintext secret values by observing length differences during a series of guesses in which a string in an HTTP request URL potentially matches an unknown string in an HTTP response body, aka a “BREACH” attack.

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-203: Observable Discrepancy

Vulnerability CVE-2022-29034

An error message pop up window in the web interface of the affected application does not prevent injection of JavaScript code.

This could allow attackers to perform reflected cross-site scripting (XSS) attacks.

CVSS v3.1 Base Score	6.1
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N/E:P/RL:O/RC:C
CWE	CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Vulnerability CVE-2022-32251

There is a missing authentication verification for a resource used to change the roles and permissions of a user. This could allow an attacker to change the permissions of any user and gain the privileges of an administrative user.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-306: Missing Authentication for Critical Function

Vulnerability CVE-2022-32252

The application does not perform the integrity check of the update packages. Without validation, an admin user might be tricked to install a malicious package, granting root privileges to an attacker.

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-345: Insufficient Verification of Data Authenticity

Vulnerability CVE-2022-32253

Due to improper input validation, the OpenSSL certificate's password could be printed to a file reachable by an attacker.

CVSS v3.1 Base Score	4.9
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2022-32254

A customized HTTP POST request could force the application to write the status of a given user to a log file, exposing sensitive user information that could provide valuable guidance to an attacker.

CVSS v3.1 Base Score	4.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-532: Insertion of Sensitive Information into Log File

Vulnerability CVE-2022-32255

The affected application consists of a web service that lacks proper access control for some of the endpoints. This could lead to unauthorized access to limited information.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-284: Improper Access Control

Vulnerability CVE-2022-32256

The affected application consists of a web service that lacks proper access control for some of the endpoints. This could lead to low privileged users accessing privileged information.

CVSS v3.1 Base Score	4.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-284: Improper Access Control

Vulnerability CVE-2022-32258

The affected application contains an older feature that allows to import device configurations via a specific endpoint. An attacker could use this vulnerability for information disclosure.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-448: Obsolete Feature in UI

Vulnerability CVE-2022-32259

The system images for installation or update of the affected application contain unit test scripts with sensitive information. An attacker could gain information about testing architecture and also tamper with test configuration.

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C
CWE	CWE-1244: Internal Asset Exposed to Unsafe Debug Access Level or State

Vulnerability CVE-2022-32261

The affected application contains a misconfiguration in the APT update. This could allow an attacker to add insecure packages to the application.

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-233: Improper Handling of Parameters

Vulnerability CVE-2022-32262

The affected application contains a file upload server that is vulnerable to command injection. An attacker could use this to achieve arbitrary code execution.

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection')

ACKNOWLEDGMENTS

Siemens thanks the following party for its efforts:

- Steffen Robertz from SEC Consult Vulnerability Lab for coordinated disclosure of CVE-2022-29034

ADDITIONAL INFORMATION

The update of SINEMA Remote Connect Server to V3.1 also contains additional fixes for vulnerabilities documented in the following Siemens Security Advisories:

- SSA-244969 (https://cert-portal.siemens.com/productcert/html/ssa-244969.html)
- SSA-539476 (https://cert-portal.siemens.com/productcert/html/ssa-539476.html)
- SSA-685781 (https://cert-portal.siemens.com/productcert/html/ssa-685781.html)
- SSA-712929 (https://cert-portal.siemens.com/productcert/html/ssa-712929.html)

Refer to the corresponding links for further details.

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 (2022-06-14):	Publication Date
V1.1 (2024-07-09):	Move CVE-2022-32260 to SSA-381581 as only fixed with SINEMA Remote Connect Server V3.2 SP1

TERMS OF USE