SSA-332410: Multiple Vulnerabilities in SINEC INS before V1.0 SP2 Update 1

Publication Date: 2023-01-10
Last Update: 2023-01-10
Current Version: V1.0
CVSS v3.1 Base Score: 9.9

SUMMARY

Siemens has released a new version for SINEC INS that fixes multiple vulnerabilities that could allow an attacker to read and write arbitrary files from the file system of the affected component and to ultimately execute arbitrary code on the device. In addition, this version also contains fixes for multiple vulnerabilities in underlying third party components.

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

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SINEC INS: All versions < V1.0 SP2 Update 1	Update to V1.0 SP2 Update 1 or later version https://support.industry.siemens.com/cs/ww/en/view/109815432/ 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:

- CVE-2022-45093: Disable the SFTP service of the affected product, if not required
- CVE-2022-45094: Disable the DHCP service of the affected product, if not required

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 INS (Infrastructure Network Services) is a web-based application that combines various network services in one tool. This simplifies installation and administration of all network services relevant for industrial 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-2022-2068

In addition to the c_rehash shell command injection identified in CVE-2022-1292, further circumstances where the c_rehash script does not properly sanitise shell metacharacters to prevent command injection were found by code review. When the CVE-2022-1292 was fixed it was not discovered that there are other places in the script where the file names of certificates being hashed were possibly passed to a command executed through the shell. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool.

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-2022-2097

AES OCB mode for 32-bit x86 platforms using the AES-NI assembly optimised implementation will not encrypt the entirety of the data under some circumstances. This could reveal sixteen bytes of data that was preexisting in the memory that wasn't written. In the special case of "in place" encryption, sixteen bytes of the plaintext would be revealed. Since OpenSSL does not support OCB based cipher suites for TLS and DTLS, they are both unaffected.

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-326: Inadequate Encryption Strength

Vulnerability CVE-2022-2274

The OpenSSL 3.0.4 release introduced a serious bug in the RSA implementation for X86_64 CPUs supporting the AVX512IFMA instructions. This issue makes the RSA implementation with 2048 bit private keys incorrect on such machines and memory corruption will happen during the computation. As a consequence of the memory corruption an attacker may be able to trigger a remote code execution on the machine performing the computation. SSL/TLS servers or other servers using 2048 bit RSA private keys running on machines supporting AVX512IFMA instructions of the X86_64 architecture are affected by this issue.

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-787: Out-of-bounds Write

Vulnerability CVE-2022-32212

A OS Command Injection vulnerability exists in Node.js versions <14.20.0, <16.16.0, <18.5.0 due to an insufficient IsAllowedHost check that can easily be bypassed because IsIPAddress does not properly check if an IP address is invalid before making DBS requests allowing rebinding attacks.

CVSS v3.1 Base Score	8.1
CVSS Vector	CVSS:3.1/AV:N/AC:H/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-2022-32213

The llhttp parser <v14.20.1, <v16.17.1 and <v18.9.1 in the http module in Node.js does not correctly parse and validate Transfer-Encoding headers and can lead to HTTP Request Smuggling (HRS).

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-444: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')

Vulnerability CVE-2022-32215

The llhttp parser <v14.20.1, <v16.17.1 and <v18.9.1 in the http module in Node.js does not correctly handle multi-line Transfer-Encoding headers. This can lead to HTTP Request Smuggling (HRS).

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-444: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')

Vulnerability CVE-2022-32222

A cryptographic vulnerability exists on Node.js on linux in versions of 18.x prior to 18.40.0 which allowed a default path for openssl.cnf that might be accessible under some circumstances to a non-admin user instead of /etc/ssl as was the case in versions prior to the upgrade to OpenSSL 3.

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-326: Inadequate Encryption Strength

Vulnerability CVE-2022-35255

Node.js made calls to EntropySource() in SecretKeyGenTraits::DoKeyGen() in src/crypto/crypto_keygen.cc. However, it does not check the return value, it assumes EntropySource() always succeeds, but it can (and sometimes will) fail.

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-330: Use of Insufficiently Random Values

Vulnerability CVE-2022-35256

The llhttp parser in the http module in Node.js v18.7.0 does not correctly handle header fields that are not terminated with CLRF. This may result in HTTP Request Smuggling.

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-290: Authentication Bypass by Spoofing

Vulnerability CVE-2022-45092

An authenticated remote attacker with access to the Web Based Management (443/tcp) of the affected product, could potentially read and write arbitrary files from and to the device's file system. An attacker might leverage this to trigger remote code execution on the affected component.

CVSS v3.1 Base Score	9.9
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Vulnerability CVE-2022-45093

An authenticated remote attacker with access to the Web Based Management (443/tcp) of the affected product as well as with access to the SFTP server of the affected product (22/tcp), could potentially read and write arbitrary files from and to the device's file system. An attacker might leverage this to trigger remote code execution on the affected component.

CVSS v3.1 Base Score	8.5
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Vulnerability CVE-2022-45094

An authenticated remote attacker with access to the Web Based Management (443/tcp) of the affected product, could potentially inject commands into the dhcpd configuration of the affected product. An attacker might leverage this to trigger remote code execution on the affected component.

CVSS v3.1 Base Score	8.4
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:H/UI:N/S:C/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')

ADDITIONAL INFORMATION

Vulnerabilities CVE-2022-45092, CVE-2022-45093, and CVE-2022-45094 have been found internally by Siemens.

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 (2023-01-10): 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.