SSA-077170: Multiple Vulnerabilities in SINEC INS before V1.0 SP2 Update 2

Publication Date: 2023-12-12
Last Update: 2023-12-12
Current Version: V1.0
CVSS v3.1 Base Score: 8.1

SUMMARY

SINEC INS before V1.0 SP2 Update 2 is affected by multiple vulnerabilities.

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 2	Update to V1.0 SP2 Update 2 or later version https://support.industry.siemens.com/cs/ww/en/view/109825710/ 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 access to application webserver for trusted users only

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-2023-0464

A security vulnerability has been identified in all supported versions of OpenSSL related to the verification of X.509 certificate chains that include policy constraints. Attackers may be able to exploit this vulnerability by creating a malicious certificate chain that triggers exponential use of computational resources, leading to a denial-of-service (DoS) attack on affected systems.

Policy processing is disabled by default but can be enabled by passing the `-policy` argument to the command line utilities or by calling the `X509_VERIFY_PARAM_set1_policies()` function.

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-295: Improper Certificate Validation

Vulnerability CVE-2023-27538

libcurl would reuse a previously created connection even when an SSH related option had been changed that should have prohibited reuse. libcurl keeps previously used connections in a connection pool for subsequent transfers to reuse if one of them matches the setup. However, two SSH settings were left out from the configuration match checks, making them match too easily.

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:H/A:N/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2023-48427

Affected products do not properly validate the certificate of the configured UMC server. This could allow an attacker to intercept credentials that are sent to the UMC server as well as to manipulate responses, potentially allowing an attacker to escalate privileges.

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-295: Improper Certificate Validation

Vulnerability CVE-2023-48428

The radius configuration mechanism of affected products does not correctly check uploaded certificates. A malicious admin could upload a crafted certificate resulting in a denial-of-service condition or potentially issue commands on system level.

CVSS v3.1 Base Score	7.2
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:H/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-2023-48429

The Web UI of affected devices does not check the length of parameters in certain conditions. This allows a malicious admin to crash the server by sending a crafted request to the server. The server will automatically restart.

CVSS v3.1 Base Score	2.7
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C
CWE	CWE-394: Unexpected Status Code or Return Value

Vulnerability CVE-2023-48430

The REST API of affected devices does not check the length of parameters in certain conditions. This allows a malicious admin to crash the server by sending a crafted request to the API. The server will automatically restart.

CVSS v3.1 Base Score	2.7
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C
CWE	CWE-392: Missing Report of Error Condition

Vulnerability CVE-2023-48431

Affected software does not correctly validate the response received by an UMC server. An attacker can use this to crash the affected software by providing and configuring a malicious UMC server or by manipulating the traffic from a legitimate UMC server (i.e. leveraging CVE-2023-48427).

CVSS v3.1 Base Score	6.8
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-754: Improper Check for Unusual or Exceptional Conditions

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 (2023-12-12): 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.