SSA-250085: Multiple Vulnerabilities in SINEC NMS

Publication Date: 2022-03-08
Last Update: 2022-03-08
Current Version: V1.0
CVSS v3.1 Base Score: 7.3

SUMMARY

SINEC NMS contains multiple vulnerabilities that could allow an attacker to execute arbitrary code on the system, arbitrary commands on the local database or achieve privilege escalation.

Siemens recommends specific countermeasures for products where updates are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SINEC NMS: All versions	Currently no remediation is available See 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 the affected systems, especially to port 443/tcp, to trusted IP addresses only
- CVE-2022-25311: If SSO was established and user is authenticated in both Control and Operation, it is recommended to logout explicitly in both Control and Operation to avoid privilege escalation

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-2022-24281

A privileged authenticated attacker could execute arbitrary commands in the local database by sending specially crafted requests to the webserver of the affected application.

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:T/RC:C
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vulnerability CVE-2022-24282

The affected system allows to upload JSON objects that are deserialized to Java objects. Due to insecure deserialization of user-supplied content by the affected software, a privileged attacker could exploit this vulnerability by sending a maliciously crafted serialized Java object. This could allow the attacker to execute arbitrary code on the device with root privileges.

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:T/RC:C
CWE	CWE-502: Deserialization of Untrusted Data

Vulnerability CVE-2022-25311

The affected software do not properly check privileges between users during the same web browser session, creating an unintended sphere of control. This could allow an authenticated low privileged user to achieve privilege escalation.

CVSS v3.1 Base Score	7.3
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-269: Improper Privilege Management

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 (2022-03-08): 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.