SSA-160243: Multiple Vulnerabilities in SINEC NMS before V2.0

Publication Date: 2023-10-10
Last Update: 2023-10-10
Current Version: V1.0
CVSS v3.1 Base Score: 7.8

SUMMARY

SINEC NMS before V2.0 is affected by a code injection and a stored cross-site scripting vulnerability.

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 < V2.0	Update to V2.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109824030/ 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-2023-44315: Restrict access to the SNMP servers in the device network
- CVE-2022-30527: Ensure that only trusted persons have access to the system and avoid the configuration of additional accounts

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-2022-30527

The affected application assigns improper access rights to specific folders containing executable files and libraries.

This could allow an authenticated local attacker to inject arbitrary code and escalate privileges.

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-732: Incorrect Permission Assignment for Critical Resource

Vulnerability CVE-2023-44315

The affected application improperly sanitizes certain SNMP configuration data retrieved from monitored devices. An attacker with access to a monitored device could prepare a stored cross-site scripting (XSS) attack that may lead to unintentional modification of application data by legitimate users.

CVSS v3.1 Base Score	4.7
CVSS Vector	CVSS:3.1/AV:N/AC:H/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')

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 (2023-10-10): 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.