SSA-078892: Multiple Vulnerabilities in SINEC NMS Before V4.0

Publication Date: 2025-07-08
Last Update: 2025-07-08
Current Version: V1.0
CVSS v3.1 Base Score: 9.8
CVSS v4.0 Base Score: 9.3

SUMMARY

Siemens SINEC NMS before V4.0 is affected by multiple vulnerabilities which could allow an attacker to elevate privilege and exceute arbitrary code.

Siemens has released a new version for SINEC NMS and recommends to update to the latest version. Siemens is preparing further fix versions and recommends countermeasures for products where fixes are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SINEC NMS: All versions < V4.0 affected by all CVEs	Update to V4.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989514/

WORKAROUNDS AND MITIGATIONS

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 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-2025-40735

The affected devices are vulnerable to SQL injection. This could allow an unauthenticated remote attacker to execute arbitrary SQL queries on the server database.

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
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Vulnerability CVE-2025-40736

The affected application exposes an endpoint that allows an unauthorized modification of administrative credentials. This could allow an unauthenticated attacker to reset the superadmin password and gain full control of the application (ZDI-CAN-26569).

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
CVSS v4.0 Base Score	9.3
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-306: Missing Authentication for Critical Function

Vulnerability CVE-2025-40737

The affected application does not properly validate file paths when extracting uploaded ZIP files. This could allow an attacker to write arbitrary files to restricted locations and potentially execute code with elevated privileges (ZDI-CAN-26571).

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
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Vulnerability CVE-2025-40738

The affected application does not properly validate file paths when extracting uploaded ZIP files. This could allow an attacker to write arbitrary files to restricted locations and potentially execute code with elevated privileges (ZDI-CAN-26572).

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
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

ACKNOWLEDGMENTS

Siemens thanks the following party for its efforts:

- Trend Micro Zero Day Initiative for coordinated disclosure of CVE-2025-40736, CVE-2025-40737, CVE-2025-40738

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 (2025-07-08): Publication Date

TERMS OF USE