

SSA-756744: OS Command Injection Vulnerability in SINEC NMS

Publication Date: 2021-08-10
Last Update: 2021-09-14
Current Version: V1.1
CVSS v3.1 Base Score: 7.2

SUMMARY

The latest update for SINEC NMS fixes a vulnerability that could allow an authenticated remote attacker to execute arbitrary code on the system, with system privileges, under certain conditions.

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 < V1.0 SP2	Update to V1.0 SP2 or later version https://support.industry.siemens.com/cs/ww/en/view/109797645/

WORKAROUNDS AND MITIGATIONS

Siemens has not identified any additional specific workarounds or mitigations. Please follow the [General Security Recommendations](#).

Product specific mitigations can be found in the section [Affected Products and Solution](#).

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-2021-33721

The affected application incorrectly neutralizes special elements when creating batch operations which could lead to command injection.

An authenticated remote attacker with administrative privileges could exploit this vulnerability to execute arbitrary code on the system with system 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:O/RC:C
CWE	CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Noam Moshe from Claroty for coordinated disclosure

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 (2021-08-10):	Publication Date
V1.1 (2021-09-14):	Updated acknowledgements

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.