SSA-128433: Multiple Vulnerabilities in SINEC NMS before V2.0 SP2

Publication Date: 2024-04-09
Last Update: 2024-04-09
Current Version: V1.0
CVSS v3.1 Base Score: 7.6
CVSS v4.0 Base Score: 7.2

SUMMARY

SINEC NMS before V2.0 SP2 is affected by multiple vulnerabilities.

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 SP2 affected by all CVEs	Update to V2.0 SP2 or later version https://support.industry.siemens.com/cs/ww/en/view/109954920/

WORKAROUNDS AND MITIGATIONS

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 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-2023-5678

Issue summary: Generating excessively long X9.42 DH keys or checking excessively long X9.42 DH keys or parameters may be very slow. Impact summary: Applications that use the functions DH_generate_key() to generate an X9.42 DH key may experience long delays. Likewise, applications that use DH_check_pub_key(), DH_check_pub_key_ex() or EVP_PKEY_public_check() to check an X9.42 DH key or X9.42 DH parameters may experience long delays. Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service. While DH_check() performs all the necessary checks (as of CVE-2023-3817), DH_check_pub_key() doesn't make any of these checks, and is therefore vulnerable for excessively large P and Q parameters. Likewise, while DH_generate_key() performs a check for an excessively large P, it doesn't check for an excessively large Q. An application that calls DH_generate_key() or DH_check_pub_key() and supplies a key or parameters obtained from an untrusted source could be vulnerable to a Denial of Service attack. DH_generate_key() and DH_check_pub_key() are also called by a number of other OpenSSL functions. An application calling any of those other functions may similarly be affected. The other functions affected by this are DH_check_pub_key_ex(), EVP_PKEY_public_check(), and EVP_PKEY_generate(). Also vulnerable are the OpenSSL pkey command line application when using the "-pubcheck" option, as well as the OpenSSL genpkey command line application. The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C
CWE	CWE-754: Improper Check for Unusual or Exceptional Conditions

Vulnerability CVE-2024-31978

Affected devices allow authenticated users to export monitoring data. The corresponding API endpoint is susceptible to path traversal and could allow an authenticated attacker to download files from the file system. Under certain circumstances the downloaded files are deleted from the file system.

CVSS v3.1 Base Score	7.6
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:H/E:P/RL:O/RC:C
CVSS v4.0 Base Score	7.2
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/VA:H/SC:N/SI:N/SA:N
CWE	CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

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 (2024-04-09): Publication Date

TERMS OF USE