SSA-928781: Multiple Vulnerabilities in SINEMA Remote Connect Server before V3.2 HF1

Publication Date: 2024-07-09
Last Update: 2024-07-09
Current Version: V1.0
CVSS v3.1 Base Score: 8.8
CVSS v4.0 Base Score: 8.7

SUMMARY

SINEMA Remote Connect Server before V3.2 HF1 is affected by multiple vulnerabilities.

Siemens has released a new version for SINEMA Remote Connect Server and recommends to update to the latest version.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SINEMA Remote Connect Server: All versions < V3.2 HF1 affected by all CVEs	Update to V3.2 HF1 or later version https://support.industry.siemens.com/cs/ww/en/view/109954687/

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

SINEMA Remote Connect is a management platform for remote networks that enables the simple management of tunnel connections (VPN) between headquarters, service technicians, and installed machines or plants. It provides both the Remote Connect Server, which is the server application, and the Remote Connect Client, which is an OpenVPN client for optimal connection to SINEMA Remote Connect Server.

 © Siemens 2024

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-2024-39570

Affected applications are vulnerable to command injection due to missing server side input sanitation when loading VxLAN configurations. This could allow an authenticated attacker to execute arbitrary code with root privileges.

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/E:P/RL:O/RC:C
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-77: Improper Neutralization of Special Elements used in a Command ('Command Injection')

Vulnerability CVE-2024-39571

Affected applications are vulnerable to command injection due to missing server side input sanitation when loading SNMP configurations. This could allow an attacker with the right to modify the SNMP configuration to execute arbitrary code with root privileges.

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/E:P/RL:O/RC:C
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-77: Improper Neutralization of Special Elements used in a Command ('Command Injection')

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 (2024-07-09): 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.