SSA-381581: Multiple Vulnerabilities in SINEMA Remote Connect Server before V3.2 SP1

Publication Date: 2024-07-09
Last Update: 2024-07-09
Current Version: V1.0
CVSS v3.1 Base Score: 9.6
CVSS v4.0 Base Score: 9.3

SUMMARY

SINEMA Remote Connect Server before V3.2 SP1 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 SP1 affected by all CVEs	Update to V3.2 SP1 or later version https://support.industry.siemens.com/cs/ww/en/view/109972765/

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.

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-2022-32260

The affected application creates temporary user credentials for UMC (User Management Component) users. An attacker could use these temporary credentials for authentication bypass in certain scenarios.

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:H/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-286: Incorrect User Management

Vulnerability CVE-2024-39865

The affected application allows users to upload encrypted backup files. As part of this backup, files can be restored without correctly checking the path of the restored file. This could allow an attacker with access to the backup encryption key to upload malicious files, that could potentially lead to remote code execution.

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-434: Unrestricted Upload of File with Dangerous Type

Vulnerability CVE-2024-39866

The affected application allows users to upload encrypted backup files. This could allow an attacker with access to the backup encryption key and with the right to upload backup files to create a user with administrative 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-267: Privilege Defined With Unsafe Actions

Vulnerability CVE-2024-39867

Affected devices do not properly validate the authentication when performing certain actions in the web interface allowing an unauthenticated attacker to access and edit device configuration information of devices for which they have no privileges.

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-425: Direct Request (’Forced Browsing’)

Vulnerability CVE-2024-39868

Affected devices do not properly validate the authentication when performing certain actions in the web interface allowing an unauthenticated attacker to access and edit VxLAN configuration information of networks for which they have no privileges.

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-425: Direct Request ('Forced Browsing')

Vulnerability CVE-2024-39869

Affected products allow to upload certificates. An authenticated attacker could upload a crafted certificates leading to a permanent denial-of-service situation. In order to recover from such an attack, the offending certificate needs to be removed manually.

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CVSS v4.0 Base Score	7.1
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N
CWE	CWE-754: Improper Check for Unusual or Exceptional Conditions

Vulnerability CVE-2024-39870

The affected applications can be configured to allow users to manage own users. A local authenticated user with this privilege could use this modify users outside of their own scope as well as to escalate privileges.

CVSS v3.1 Base Score	6.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C
CVSS v4.0 Base Score	7.1
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N
CWE	CWE-602: Client-Side Enforcement of Server-Side Security

Vulnerability CVE-2024-39871

Affected applications do not properly separate the rights to edit device settings and to edit settings for communication relations. This could allow an authenticated attacker with the permission to manage devices to gain access to participant groups that the attacked does not belong to.

CVSS v3.1 Base Score	6.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C
CVSS v4.0 Base Score	5.3
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N
CWE	CWE-863: Incorrect Authorization

Vulnerability CVE-2024-39872

The affected application does not properly assign rights to temporary files created during its update process. This could allow an authenticated attacker with the 'Manage firmware updates' role to escalate their privileges on the underlying OS level.

CVSS v3.1 Base Score	9.6
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:N/E:P/RL:O/RC:C
CVSS v4.0 Base Score	9.3
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:N/SC:N/SI:H/SA:H
CWE	CWE-378: Creation of Temporary File With Insecure Permissions

Vulnerability CVE-2024-39873

The affected application does not properly implement brute force protection against user credentials in its web API. This could allow an attacker to learn user credentials that are vulnerable to brute force attacks.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/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:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N
CWE	CWE-307: Improper Restriction of Excessive Authentication Attempts

Vulnerability CVE-2024-39874

The affected application does not properly implement brute force protection against user credentials in its Client Communication component. This could allow an attacker to learn user credentials that are vulnerable to brute force attacks.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/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:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N
CWE	CWE-307: Improper Restriction of Excessive Authentication Attempts

Vulnerability CVE-2024-39875

The affected application allows authenticated, low privilege users with the ‘Manage own remote connections’ permission to retrieve details about other users and group memberships.

CVSS v3.1 Base Score	4.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
CVSS v4.0 Base Score	5.3
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N
CWE	CWE-732: Incorrect Permission Assignment for Critical Resource

Vulnerability CVE-2024-39876

Affected applications do not properly handle log rotation. This could allow an unauthenticated remote attacker to cause a denial of service condition through resource exhaustion on the device.

CVSS v3.1 Base Score	4.0
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C
CVSS v4.0 Base Score	5.3
CVSS Vector	CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N
CWE	CWE-770: Allocation of Resources Without Limits or Throttling

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