SSA-334944: Vulnerability in SINEMA Remote Connect Server

Publication Date: 2021-09-14
Last Update: 2021-09-14
Current Version: V1.0
CVSS v3.1 Base Score: 7.4

SUMMARY

Multiple vulnerabilities in SINEMA Remote Connect Server could allow an unauthorized remote attacker to retrieve or manipulate sensitive information from the affected software. In addition, the attacker could also cause a Denial-of-Service condition in devices controlled by the affected software.

Siemens has released an update for the 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 < V3.0 SP2	Update to V3.0 SP2 or later version https://support.industry.siemens.com/cs/de/en/view/109793790/

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

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 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-2021-37177

The status provided by the syslog clients managed by the affected software can be manipulated by an unauthenticated attacker in the same network of the affected system.

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N/E:P/RL:O/RC:C
CWE	CWE-471: Modification of Assumed-Immutable Data (MAID)

Vulnerability CVE-2021-37183

The affected software allows sending send-to-sleep notifications to the managed devices. An unauthenticated attacker in the same network of the affected system can abuse these notifications to cause a Denial-of-Service condition in the managed devices.

CVSS v3.1 Base Score	7.4
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-284: Improper Access Control

Vulnerability CVE-2021-37190

The affected software has an information disclosure vulnerability that could allow an attacker to retrieve VPN connection for a known user.

CVSS v3.1 Base Score	4.3
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

Vulnerability CVE-2021-37191

An unauthenticated attacker in the same network of the affected system could brute force the usernames from the affected software.

CVSS v3.1 Base Score	3.1
CVSS Vector	CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-799: Improper Control of Interaction Frequency

Vulnerability CVE-2021-37192

The affected software has an information disclosure vulnerability that could allow an attacker to retrieve a list of network devices a known user can manage.

CVSS v3.1 Base Score	4.3
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

Vulnerability CVE-2021-37193

An unauthenticated attacker in the same network of the affected system could manipulate certain parameters and set a valid user of the affected software as invalid (or vice-versa).

CVSS v3.1 Base Score	4.3
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N/E:P/RL:O/RC:C
CWE	CWE-471: Modification of Assumed-Immutable Data (MAID)

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Cybersecurity and Infrastructure Security Agency (CISA) for coordination efforts
- Sharon Brizinov 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 (2021-09-14):	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.