SSA-653855: Information Disclosure vulnerability in SINEMA Remote Connect Client before V3.1 SP1

Publication Date:	2024-03-12
Last Update:	2024-03-12
Current Version:	V1.0
CVSS v3.1 Base Score:	7.6
CVSS v4.0 Base Score:	6.1

SUMMARY

SINEMA Remote Connect Client before V3.1 SP1 is affected by an information disclosure vulnerability.

Siemens has released updates for the affected products and recommends to update to the latest versions.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SINEMA Remote Connect Client: All versions < V3.1 SP1 affected by all CVEs	Update to V3.1 SP1 or later version In order to fully mitigate the issue, administrators are advised to backup and clear the log files and to change the VPN credentials. https://support.industry.siemens.com/cs/ww/en/view/109817939/

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-2024-22045

The product places sensitive information into files or directories that are accessible to actors who are allowed to have access to the files, but not to the sensitive information. This information is also available via the web interface of the product.

CVSS v3.1 Base Score	7.6
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:L/A:N/E:P/RL:O/RC:C
CVSS v4.0 Base Score	6.1
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:P/VC:N/VI:N/VA:N/SC:H/SI:L/SA:N
CWE	CWE-538: Insertion of Sensitive Information into Externally-Accessible File or Directory

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 (2024-03-12):	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.