

SSA-654775: Open Redirect Vulnerability in SINEMA Remote Connect Server

Publication Date: 2022-02-08
Last Update: 2022-02-08
Current Version: V1.0
CVSS v3.1 Base Score: 5.4

SUMMARY

An open redirect vulnerability in SINEMA Remote Connect Server could allow an attacker to steal logon credentials with a specially crafted malicious link.

Siemens has released software 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 < V2.0	Update to V2.0 or later version https://support.industry.siemens.com/cs/document/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-2022-23102

Affected products contain an open redirect vulnerability.

An attacker could trick a valid authenticated user to the device into clicking a malicious link there by leading to phishing attacks.

CVSS v3.1 Base Score	5.4
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C
CWE	CWE-601: URL Redirection to Untrusted Site ('Open Redirect')

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- SEC Consult Vulnerability Lab 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 (2022-02-08): 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.