SSA-816035: Code Execution Vulnerability in SINEMA Remote Connect Client

Publication Date: 2021-08-19
Last Update: 2021-08-19
Current Version: V1.0
CVSS v3.1 Base Score: 7.8

SUMMARY

The latest update for SINEMA Remote Connect Client fixes a vulnerability that could allow a local attacker to escalate privileges or even allow remote code execution under certain circumstances.

Siemens has released a firmware update for SINEMA Remote Connect Client and proposes mitigations if an update is not possible.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SINEMA Remote Connect Client: All versions < V3.0 SP1	Update to V3.0 SP1 or later version https://support.industry.siemens.com/cs/de/en/view/109793790/

WORKAROUNDS AND MITIGATIONS

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- Do not access links from untrusted sources
- Restrict access to hosts running SINEMA Remote Connect Client to trusted personnel

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-2021-31338

Affected devices allow to modify configuration settings over an unauthenticated channel.

This could allow a local attacker to escalate privileges and execute own code on the device.

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-15: External Control of System or Configuration Setting

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Amir Preminger 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 (2021-08-19): Publication Date

TERMS OF USE