SSA-731317: Multiple vulnerabilities in SINEMA Remote Connect Web Based Management

Publication Date: 2021-03-09
Last Update: 2021-03-09
Current Version: V1.0
CVSS v3.1 Base Score: 8.8

SUMMARY

The latest update for SINEMA Remote Connect Server fixes vulnerabilities in the web interface that could allow authenticated unpriviledged user accounts to access functionality unauthorized. Siemens has released updates for SINEMA Remote Connect Server and recommends specific countermeasures.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SINEMA Remote Connect Server: All versions < V3.0	Update to V3.0 https://support.industry.siemens.com/cs/ww/en/view/109793790

WORKAROUNDS AND MITIGATIONS

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

- Check that all settings are as expected when applying templates
- Configure a syslog server for logs
- Ensure that all (including unprivileged) accounts are trusted

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 ensures management of secure connections (VPN) between headquarters, service technicians and the installed machines or plants.

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-2020-25239

The webserver could allow unauthorized actions via special urls for unpriviledged users. The settings of the UMC authorization server could be changed to add a rogue server by an attacker authenticating with unprivilege user rights.

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
CWE	CWE-863: Incorrect Authorization

Vulnerability CVE-2020-25240

Unpriviledged users can access services when guessing the url. An attacker could impact availability, integrity and gain information from logs and templates of the service.

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:U/RC:C
CWE	CWE-863: Incorrect Authorization

ADDITIONAL INFORMATION

This vulnerability has been discovered internally by Siemens.

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 (2021-03-09): Publication Date

TERMS OF USE