SSA-884497: Multiple Vulnerabilities in SINEMA Remote Connect Server

Publication Date: 2019-09-10
Last Update: 2019-09-10
Current Version: V1.0
CVSS v3.0 Base Score: 8.1

SUMMARY

The latest update for SINEMA Remote Connect Server fixes four vulnearbilities in the web interface. Two of the vulnerabilities are missing protection mechanisms for password guessing and for Cross Site Request Forgery attacks, the third one is a missing authentication check, and the fourth one could allow an attacker with administrative privileges to obtain a device password hash.

Siemens has released updates and recommends to update to the newest version.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SINEMA Remote Connect Server: All versions < V2.0 SP1	Update to V2.0 SP1 https://support.industry.siemens.com/cs/ww/en/view/109770899

WORKAROUNDS AND MITIGATIONS

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

- Restrict network access to the SINEMA Remote Connect web interface
- Do not access links from untrusted sources while logged in at SINEMA Remote Connect

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 3.0 (CVSS v3.0) (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.

Vulnerability CVE-2019-13918

The web interface has no means to prevent password guessing attacks.

The vulnerability could be exploited by an attacker with network access to the vulnerable software, requiring no privileges and no user interaction. The vulnerability could allow full access to the web interface.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.0 Base Score	8.1
CVSS Vector	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C

Vulnerability CVE-2019-13919

Some pages that should only be accessible by a privileged user can also be accessed by a non-privileged user.

The security vulnerability could be exploited by an attacker with network access and valid credentials for the web interface. No user interaction is required. The vulnerability could allow an attacker to access information that he should not be able to read. The affected information does not include passwords.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.0 Base Score	4.3
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C

Vulnerability CVE-2019-13920

Some parts of the web application are not protected against Cross Site Request Forgery (CSRF) attacks.

The security vulnerability could be exploited by an attacker that is able to trigger requests of a logged-in user to the application. The vulnerability could allow switching the connectivity state of a user or a device.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.0 Base Score	3.4
CVSS Vector	CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:N/I:L/A:N/E:P/RL:O/RC:C

Vulnerability CVE-2019-13922

An attacker with administrative privileges can obtain the hash of a connected device's password.

The security vulnerability could be exploited by an attacker with network access to the SINEMA Remote Connect Server and administrative privileges.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.0 Base Score	6.6
CVSS Vector	CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:C/C:N/I:L/A:H/E:P/RL:O/RC:C

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Hendrik Derre and Tijl Deneut from HOWEST 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 (2019-09-10): Publication Date

TERMS OF USE