SSA-880233: Incorrect Session Validation Vulnerability in SINEMA Server

Publication Date: 2020-01-14
Last Update: 2020-01-14
Current Version: V1.0
CVSS v3.1 Base Score: 9.9

SUMMARY

The latest update for SINEMA Server fixes a vulnerability that could allow authenticated users with a low-privileged account to perform firmware updates (as well as other administrative operations) on connected devices. Therefore, Siemens recommends to update the affected products.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SINEMA Server: All versions < V14.0 SP2 Update 1	Update to V14.0 SP2 Update 1 https://support.industry.siemens.com/cs/ww/en/view/109773579

WORKAROUNDS AND MITIGATIONS

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

- Restrict network access to device port 443/tcp to trusted IP addresses.
- Restrict low-privileged accounts access to trusted persons.

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 Server is a network management software designed by Siemens for use in Industrial Ethernet networks.

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-2019-10940

Incorrect session validation could allow an attacker with a valid session, with low privileges, to perform firmware updates and other administrative operations on connected devices.

The security vulnerability could be exploited by an attacker with network access to the affected system. An attacker must have access to a low privileged account in order to exploit the vulnerability. An attacker could use the vulnerability to compromise confidentiality, integrity, and availability of the affected system and underlying components.

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

CVSS v3.1 Base Score	9.9
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-266: Incorrect Privilege Assignment

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Antonin Rahon from Agilicom for reporting the vulnerability

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 (2020-01-14): Publication Date

TERMS OF USE