# SSA-835377: Missing Authentication Vulnerability in SINEMA Server

Publication Date: 2021-09-14
Last Update: 2021-09-14
Current Version: V1.0
CVSS v3.1 Base Score: 4.7

## SUMMARY

The latest update for SINEMA Server fixes a vulnerability that could allow an unauthenticated attacker to obtain encoded system configuration backup files under certain conditions.

Siemens has released an update for the SINEMA Server and recommends to update to the latest version.

## AFFECTED PRODUCTS AND SOLUTION

| Affected Product and Versions | Remediation |
|---|---|
| SINEMA Server:<br>All versions < V14 SP3 | Update to V14 SP3 or later version<br>https://support.industry.siemens.com/cs/ww/en/view/109801374/ |

## WORKAROUNDS AND MITIGATIONS

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

- Monitor and restrict network access to device port 443/tcp and 80/tcp to trusted IP addresses
- Consider adding to your monitoring capabilities an allowed time window for system configuration backup download. This will be an auxiliar to create a baseline and monitor for abnormal behavior

## 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 monitoring and 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-2019-10941

Missing authentication for functionality that requires administrative user identity could allow an attacker to obtain encoded system configuration backup files. This is only possible through network access to the affected system, and successful exploitation requires no system privileges.

| | |
|---|---|
| CVSS v3.1 Base Score | 4.7 |
| CVSS Vector | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:N/A:N/E:P/RL:O/RC:C |
| CWE | CWE-306: Missing Authentication for Critical Function |

## 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 (2021-09-14): | 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.