# SSA-594373: Cross-Site-Scripting (XSS) Vulnerability in SINEMA Server V14

Publication Date: 2023-10-10
Last Update: 2023-10-10
Current Version: V1.0
CVSS v3.1 Base Score: 8.3

## SUMMARY

SINEMA Server V14 improperly sanitizes certain SNMP configuration data retrieved from monitored devices. An attacker with access to a monitored device could perform a stored cross-site scripting (XSS) attack that may lead to arbitrary code execution with `SYSTEM` privileges on the application server.

Siemens recommends to migrate to its successor product SINEC NMS V2.0 or later. Siemens recommends to apply specific countermeasures for products where updates are not, or not yet available.

## AFFECTED PRODUCTS AND SOLUTION

| Affected Product and Versions | Remediation |
|---|---|
| SINEMA Server V14:<br>All versions | Currently no fix is planned<br>See recommendations from section Workarounds and Mitigations |

## WORKAROUNDS AND MITIGATIONS

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

- Restrict access to the SNMP servers in the device network

Please follow the General Security Recommendations.

## 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

SINEC NMS is a new generation of the Network Management System (NMS) for the Digital Enterprise. This system can be used to centrally monitor, manage, and configure networks.

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-2023-35796

The affected application improperly sanitizes certain SNMP configuration data retrieved from monitored devices. An attacker with access to a monitored device could perform a stored cross-site scripting (XSS) attack that may lead to arbitrary code execution with `SYSTEM` privileges on the application server. (ZDI-CAN-19823)

| | |
|---|---|
| CVSS v3.1 Base Score | 8.3 |
| CVSS Vector | CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H/E:P/RL:U/RC:C |
| CWE | CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') |

## ACKNOWLEDGMENTS

Siemens thanks the following party for its efforts:

- Trend Micro Zero Day Initiative for coordinated disclosure

## ADDITIONAL INFORMATION

SINEMA Server V14 has already reached end of software support. Siemens recommends to use SINEC NMS V2.0 or later instead.

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 (2023-10-10): Publication Date

## TERMS OF USE