SSA-156833: Zip-Slip Directory Traversal Vulnerability in SINEMA Server and SINEC NMS

Publication Date: 2021-02-09
Last Update: 2021-02-09
Current Version: V1.0
CVSS v3.1 Base Score: 8.8

SUMMARY

There exists a directory traversal vulnerability which allows arbitrary file upload to an affected system. This type of vulnerability is also known as 'Zip-Slip'. An authenticated attacker could exploit this vulnerability to gain arbitrary code execution by uploading a new or modifying an existing file to an affected system.

Siemens has released updates for the affected products and recommends to update to the latest versions.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SINEC NMS: All versions < V1.0 SP1 Update 1	Update to V1.0 SP1 Update 1 or later version https://support.industry.siemens.com/cs/ww/en/view/109792922/
SINEMA Server: All versions < V14.0 SP2 Update 2	Update to V14.0 SP2 Update 2 or later version https://support.industry.siemens.com/cs/ww/en/view/109792920/

WORKAROUNDS AND MITIGATIONS

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

- Restrict access to the affected components to trusted personnel.

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-2020-25237

When uploading files to an affected system using a zip container, the system does not correctly check if the relative file path of the extracted files is still within the intended target directory. With this an attacker could create or overwrite arbitrary files on an affected system. This type of vulnerability is also known as 'Zip-Slip'. (ZDI-CAN-12054)

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:U/RC:C
CWE	CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Trend Micro Zero Day Initiative for coordinated disclosure
- Cybersecurity and Infrastructure Security Agency (CISA) for coordination efforts

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 (2021-02-09): Publication Date

TERMS OF USE