SSA-321174: Privilege Escalation in SINEMA Server

Publication Date 2016-08-02
Last Update 2016-10-12
Current Version V1.1
CVSS v3.0 Base Score 7.3

SUMMARY

SINEMA Server is affected by a vulnerability that could allow authenticated operating system users to escalate their privileges under certain conditions.

Siemens provides a new version of SINEMA Server which fixes the vulnerability, and recommends all users update to the new version.

AFFECTED PRODUCTS

SINEMA Server: All versions < V13 SP2

DESCRIPTION

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

Detailed information about the vulnerability is provided below.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.0 (CVSS v3.0) (http://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 assessed by the customer to accomplish final scoring.

Vulnerability Description (CVE-2016-6486)

The file permissions set for the SINEMA Server application folder could allow authenticated operating system users to escalate their privileges.

CVSS Base Score 7.3
CVSS Vector CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C

SOLUTION

Siemens provides SINEMA Server V13 SP2 [1] which fixes the vulnerability and recommends customers update to the new version.

As a general security measure Siemens strongly recommends to protect network access to SINEMA Server with appropriate mechanisms. It is advised to configure the environment according to our operational guidelines [2] in order to run the devices in a protected IT environment.

ACKNOWLEDGEMENTS

Siemens thanks the following for their support and efforts:

- rgod working with Trend Micro’s Zero Day Initiative for coordinated disclosure of the vulnerability.
- Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) for reporting the vulnerability and coordination efforts.

ADDITIONAL RESOURCES

[1] SINEMA Server V13 SP2 can be downloaded here:
https://support.industry.siemens.com/cs/ww/en/view/109741833

[2] An overview of the operational guidelines for Industrial Security (with the cell protection concept):
https://www.siemens.com/cert/operational-guidelines-industrial-security

[3] Information about Industrial Security by Siemens:
https://www.siemens.com/industrialsecurity

[4] For further inquiries on vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:
https://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2016-08-02): Publication Date
V1.1 (2016-10-12): Published new version

DISCLAIMER