SSA-119132: Cross-Site Scripting Vulnerability in SINEMA Remote Connect Server

Publication Date 2016-07-22
Last Update 2016-07-22
Current Version V1.0
CVSS v3.0 Base Score 4.7

SUMMARY

Siemens released version V1.2 of SINEMA Remote Connect Server that fixes a vulnerability which could allow cross-site scripting attacks under certain conditions.

AFFECTED PRODUCTS

SINEMA Remote Connect Server: All versions < V1.2

DESCRIPTION

SINEMA Remote Connect ensures management of secure connections (VPN) between headquarters, service technicians and the installed machines or plants.

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 (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 defined by the customer to accomplish final scoring.

Vulnerability Description (CVE-2016-6204)

The integrated web server (port 443/tcp) of the affected SINEMA Remote Connect Server could allow Cross-Site Scripting (XSS) attacks if unsuspecting users are tricked into accessing a malicious link.

CVSS Base Score 4.7
CVSS Vector CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:N/A:N/E:P/RL:O/RC:C

Mitigating Factors

Attackers can only take advantage of the vulnerability if they are able to trick users into accessing a malicious link.

SOLUTION

Siemens provides software update V1.2 [1] for SINEMA Remote Connect Server which fixes the vulnerability and recommends customers to update to the new version.

As a general security measure Siemens strongly recommends to configure the environment according to our operational guidelines [2].

ACKNOWLEDGEMENTS

Siemens thanks the following for their support and efforts:

- Antonio Morales Maldonado from INNOTEC SYSTEM, for coordinated disclosure of the vulnerability.
- Alexander Van Maele and Tijl Deneut from Howest for coordinated disclosure of the vulnerability.

ADDITIONAL RESOURCES

[1] The software update for SINEMA Remote Connect Server can be obtained at:
https://support.industry.siemens.com/cs/ww/en/view/109737963

[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 (2016-07-22): Publication Date

DISCLAIMER