SSA-436177: Multiple Vulnerabilities in SINEMA Remote Connect

Publication Date: 2019-04-09
Last Update: 2019-04-09
Current Version: V1.0
CVSS v3.0 Base Score: 8.3

SUMMARY

The latest updates for SINEMA Remote Connect Client and Server fix multiple vulnerabilities. One of these vulnerabilities could allow an attacker to circumvent the authorization of the system for certain functionalities and to execute privileged functions.

Siemens has released firmware updates for SINEMA Remote Connect Client and Server.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SINEMA Remote Connect Client: All versions < V2.0 HF1 only affected by CVE-2018-14618, CVE-2018-16890, CVE-2019-3822	Update to V2.0 HF1 https://support.industry.siemens.com/cs/de/en/view/109764829
SINEMA Remote Connect Server: All versions < V2.0 only affected by CVE-2019-6570	Update to V2.0 https://support.industry.siemens.com/cs/de/en/view/109764829

WORKAROUNDS AND MITIGATIONS

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

- Turn off NTLM authentication to mitigate CVE-2018-16890 and CVE-2019-3822.
- Turn off SMTP to mitigate CVE-2019-3823.
- Apply appropriate strategies for mitigation.

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

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.0 (CVSS v3.0) (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.

Vulnerability CVE-2018-14618

The HTTP client curl is vulnerable to a buffer overrun.

The security vulnerability could be exploited by an attacker providing a malicious HTTP server. Successful exploitation requires no system privileges. User interaction by a legitimate user is required in order to exploit the vulnerability. An attacker could use the vulnerability to compromise confidentiality, integrity and availability of the device.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.0 Base Score	7.5
CVSS Vector	CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

Vulnerability CVE-2018-16890

The HTTP client library libcurl is vulnerable to a heap buffer out-of-bounds read.

The security vulnerability could be exploited by an attacker providing a malicious HTTP server. Successful exploitation requires no system privileges and no user interaction. An attacker could use the vulnerability to compromise availability of the affected system.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.0 Base Score	7.5
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C

Vulnerability CVE-2019-3822

The HTTP client library libcurl is vulnerable to a stack-based buffer overflow.

The security vulnerability could be exploited by an attacker providing a malicious HTTP server. Successful exploitation requires no system privileges and no user interaction. An attacker could use the vulnerability to compromise confidentiality, integrity and availability of the affected system.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.0 Base Score	8.1
CVSS Vector	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

Vulnerability CVE-2019-6570

Due to insufficient checking of user permissions, an attacker may access URLs that require special authorization.

The security vulnerability could be exploited by an attacker with network access to the affected system. An attacker must have access to a low privileged account in order to exploit the vulnerability. An attacker could use the vulnerability to compromise confidentiality, integrity and availability of the affected system.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.0 Base Score	8.3
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:H/E:P/RL:O/RC:C

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 (2019-04-09): Publication Date

TERMS OF USE