SSA-436177: Multiple Vulnerabilities in SINEMA Remote Connect

Publication Date: 2019-04-09
Last Update: 2021-03-09
Current Version: V1.1
CVSS v3.1 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, CVE-2019-3823	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

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

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 3.1 (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-2018-14618

The libcurl library versions 7.15.4 to and including 7.61.0 are vulnerable to a buffer overrun. The flaw is caused by an improper calculation of the required buffer size in the Curl_ntlm_core_mk_nt_hash function of libcurl.

The security vulnerability could be exploited by an attacker providing a malicious HTTP server.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C
CWE	CWE-131: Incorrect Calculation of Buffer Size

Vulnerability CVE-2018-16890

The libcurl library versions 7.34.0 to and including 7.63.0 are vulnerable to a heap buffer out-of-bounds read.

The security vulnerability could be exploited by an attacker providing a malicious HTTP server.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2019-3822

The libcurl library versions 7.34.0 to and including 7.63.0 are vulnerable to a stack-based buffer overflow.

The security vulnerability could be exploited by an attacker providing a malicious HTTP server.

CVSS v3.1 Base Score	8.1
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-121: Stack-based Buffer Overflow

Vulnerability CVE-2019-3823

The libcurl library versions 7.34.0 to and including 7.63.0 are vulnerable to a heap out-of-bounds read in the code handling the end-of-response for SMTP.

This vulnerability could allow an attacker to trigger a Denial-of-Service condition on the affected devices.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2019-6570

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

An attacker must have access to a low privileged account in order to exploit the vulnerability.

CVSS v3.1 Base Score	8.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-280: Improper Handling of Insufficient Permissions or Privileges

ADDITIONAL INFORMATION

Impact of libcurl vulnerabilities to other Siemens products:

- Siemens Security Advisory SSA-936080

For more details regarding the libcurl vulnerability refer to:

- Project curl Security Advisory “NTLM type-2 out-of-bounds buffer read”
- Project curl Security Advisory “NTLMv2 type-3 header stack buffer overflow”
- Project curl Security Advisory “SMTP end-of-response out-of-bounds read”

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
V1.1 (2021-03-09): Added CVE-2019-3823

TERMS OF USE