SSA-936080: Multiple Vulnerabilities in Third-Party Component libcurl

Publication Date: 2021-03-09
Last Update: 2021-09-14
Current Version: V1.2
CVSS v3.1 Base Score: 7.5

SUMMARY

SIMATIC CM 1542-1, SCALANCE SC600 family and SIMATIC CP 343-1 Advanced devices are vulnerable to a vulnerability in the third party component libcurl that could allow an attacker to cause a Denial-of-Service condition on the affected devices.

Siemens has released updates for several affected products and recommends to update to the latest versions. Siemens recommends specific countermeasures for products where updates are not, or not yet available.

The impact of additional libcurl vulnerabilities is described in Siemens Security Advisory SSA-436177.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SCALANCE SC600 Family: All versions < V2.0	Update to V2.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109769665/
SIMATIC CM 1542-1: All versions < V3.0	Update to V3.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109801629/
SIMATIC CP 343-1 Advanced (incl. SIPLUS variants): V3.0.33, V3.0.44 and V3.0.53	See recommendations from section Workarounds and Mitigations

WORKAROUNDS AND MITIGATIONS

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

- Disable the SMTP Client function on affected devices or use VPN for protecting SMTP traffic to trusted email servers only

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

Communication Processor (CP) modules of families SIMATIC CP 343-1 and CP 443-1 have been designed to enable SIMATIC S7-300/S7-400 CPUs for Ethernet communication.

The SCALANCE SC-600 devices (SC622-2C, SC632-2C, SC636-2C, SC642-2C, SC646-2C) are used to protect trusted industrial networks from untrusted networks. They allow filtering incoming and outgoing network connections in different ways.

The SIMATIC CM 1542-1 communication module is used to connect S7-1500 controllers to PROFINET as IO-Controller.

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-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

ADDITIONAL INFORMATION

Impact of other libcurl vulnerabilities to Siemens products:

- Siemens Security Advisory SSA-436177

For more details regarding the libcurl vulnerability refer to:

- 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 (2021-03-09): Publication Date
V1.1 (2021-05-11): Added SIMATIC CP 343-1 Advanced (incl. SIPLUS variants) to the list of affected products
V1.2 (2021-09-14): Added solution for SIMATIC CM 1542-1

TERMS OF USE