SSA-200951: Multiple Vulnerabilities in Third-Party Component libcurl of TIM Devices

Publication Date: 2021-06-08
Last Update: 2021-06-08
Current Version: V1.0
CVSS v3.1 Base Score: 7.5

SUMMARY

SIMATIC TIM 1531 IRC devices are vulnerable to multiple vulnerabilities in the third party component libcurl that could allow an attacker to extract sensitive information and pass a revoked certificate as valid.

Siemens has released an update for SIMATIC TIM 1531 IRC and recommends to update to the latest versions.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC TIM 1531 IRC (incl. SIPLUS NET variants): All versions < V2.2	Update to V2.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109798331/

WORKAROUNDS AND MITIGATIONS

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

- Restrict access to the device to the internal or VPN network and to trusted IP addresses 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

TIM 1531 IRC is a communication module for SIMATIC S7-1500, S7-400, S7-300 with SINAUT ST7, DNP3 and IEC 60870-5-101/104 with three RJ45 interfaces for communication via IP-based networks (WAN / LAN) and a RS 232/RS 485 interface for communication via classic WAN networks.

SIPLUS extreme products are designed for reliable operation under extreme conditions and are based on SIMATIC, LOGO!, SITOP, SINAMICS, SIMOTION, SCALANCE or other devices. SIPLUS devices use the same firmware as the product they are based on.

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-2020-8169

The libcurl library versions 7.62.0 to and including 7.70.0 are vulnerable to an information disclosure vulnerability that can lead to a partial password being leaked over the network and to the DNS server(s).

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C
CWE	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

Vulnerability CVE-2020-8286

The libcurl library versions 7.41.0 to and including 7.73.0 are vulnerable to an improper check for certificate revocation due to insufficient verification of the OCSP response. This vulnerability could allow an attacker to pass a revoked certificate as valid.

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:H/A:N/E:U/RL:O/RC:C
CWE	CWE-295: Improper Certificate Validation

ADDITIONAL INFORMATION

For more details regarding the libcurl vulnerabilities refer to:

- Project curl Security Advisory "Partial password leak over DNS on HTTP redirect"
- Project curl Security Advisory "Inferior OCSP verification"

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 (2021-06-08): Publication Date

TERMS OF USE