SSA-316383: NumberJack Vulnerability in LOGO! CMR family and SIMATIC RTU 3000 family

Publication Date: 2021-09-14
Last Update: 2021-09-14
Current Version: V1.0
CVSS v3.1 Base Score: 5.4

SUMMARY

A vulnerability has been identified in the underlying TCP/IP stack of LOGO! CMR family and SIMATIC RTU 3000 family devices. It could allow an attacker with network access to the LAN interface of an affected device to hijack an ongoing connection or spoof a new one. The WAN interface, however, is not affected.

Siemens has released an update for the LOGO! CMR family and recommends to update to the latest version. Siemens is preparing further updates and recommends countermeasures for products where updates are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
LOGO! CMR2020: All versions < V2.2	Update to V2.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109800267/
LOGO! CMR2040: All versions < V2.2	Update to V2.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109800267/
SIMATIC RTU 3000 family: All versions	See recommendations from section Workarounds and Mitigations

WORKAROUNDS AND MITIGATIONS

Siemens has not identified any additional specific workarounds or mitigations. Please follow the General Security Recommendations.

Product specific mitigations can be found in the section Affected Products and Solution.

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

The devices of the LOGO! CMR family (in combination with the LOGO! logic module) are cost-efficient communication systems suitable for monitoring and controlling distributed plants and systems via text message or email. LOGO! CMR devices can send text messages or emails to predefined mobile network numbers as well as receive text messages from predefined mobile network numbers. The LOGO! CMR devices offer comfortable Web Based Management commissioning and diagnostics via local and/or remote access.

The devices of the RTU3000C family are compact telecontrol stations for applications with their own power supply for autonomous energy systems. They are particularly suited for monitoring and control of external stations that are not connected to an energy supply network. The RTUs can autonomously record data with time stamp from connected sensors, pre-process this data and transfer it to a control center.

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-2021-37186

The underlying TCP/IP stack does not properly calculate the random numbers used as ISN (Initial Sequence Numbers). An adjacent attacker with network access to the LAN interface could interfere with traffic, spoof the connection and gain access to sensitive information.

CVSS v3.1 Base Score	5.4
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N/E:U/RL:O/RC:C
CWE	CWE-330: Use of Insufficiently Random Values

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 (2021-09-14): Publication Date

TERMS OF USE

Siemens Security Advisories are subject to the terms and conditions contained in Siemens' underlying license terms or other applicable agreements previously agreed to with Siemens (hereinafter "License Terms"). To the extent applicable to information, software or documentation made available in or through a Siemens Security Advisory, the Terms of Use of Siemens' Global Website (https://www.siemens.com/terms_of_use, hereinafter "Terms of Use"), in particular Sections 8-10 of the Terms of Use, shall apply additionally. In case of conflicts, the License Terms shall prevail over the Terms of Use.