SSA-647068: Ripple20 in SIMATIC RTLS Gateways

Publication Date: 2024-02-13
Last Update: 2024-02-13
Current Version: V1.0
CVSS v3.1 Base Score: 7.5
CVSS v4.0 Base Score: 7.7

SUMMARY

SIMATIC RTLS Gateways are affected by vulnerabilities that were disclosed by JSOF research lab "Ripple20" for the TCP/IP stack.

Siemens recommends countermeasures for products where fixes are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC RTLS Gateway RTLS4030G, CMIIT (6GT2701-5DB23): All versions affected by all CVEs	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC RTLS Gateway RTLS4030G, ETSI (6GT2701-5DB03): All versions affected by all CVEs	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC RTLS Gateway RTLS4030G, FCC (6GT2701-5DB13): All versions affected by all CVEs	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC RTLS Gateway RTLS4030G, ISED (6GT2701-5DB33): All versions affected by all CVEs	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC RTLS Gateway RTLS4430G, Chirp, ETSI, FCC, ISED, IP65 (6GT2701-5CB03): All versions affected by all CVEs	Currently no fix is planned 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:

- Implement Security recommendations according to the product manual

Please follow the General Security Recommendations.

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

SIMATIC RTLS is a real-time wireless locating system for flexible and cost-effective locating solutions. It allows to navigate material flows, control mobile robots, monitor the use of components, and document the assembly of the end product.

VULNERABILITY DESCRIPTION

This chapter describes all vulnerabilities (CVE-IDs) addressed in this security advisory. Wherever applicable, it also documents the product-specific impact of the individual vulnerabilities.

Vulnerability CVE-2020-11896

The Treck TCP/IP stack on affected devices improperly handles length parameter inconsistencies. Unauthenticated remote attackers may be able to send specially crafted IP packets which could lead to a denial of service condition or remote code execution.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CVSS v4.0 Base Score	7.7
CVSS Vector	CVSS:4.0/AV:A/AC:H/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-130: Improper Handling of Length Parameter Inconsistency

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 (2024-02-13): 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.