SSA-480937: Denial of Service Vulnerability in CP 44x-1 RNA before V1.5.18

Publication Date: 2022-05-10
Last Update: 2022-05-10
Current Version: V1.0
CVSS v3.1 Base Score: 7.4

SUMMARY

Siemens has released a new version for the communication processor modules CP 44x-1 RNA that fixes a vulnerability that could allow an attacker to cause a denial of service condition.

Siemens has released updates for the affected products and recommends to update to the latest versions.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC CP 442-1 RNA (6GK7442-1RX00-0XE0): All versions < V1.5.18	Update to V1.5.18 or later version https://support.industry.siemens.com/cs/ww/en/view/109808794/
SIMATIC CP 443-1 RNA (6GK7443-1RX00-0XE0): All versions < V1.5.18	Update to V1.5.18 or later version https://support.industry.siemens.com/cs/ww/en/view/109808796/

WORKAROUNDS AND MITIGATIONS

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

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

The Communication Processor (CP) of the Redundant Network Access (RNA) series have been designed to connect SIMATIC S7-400 CPUs to Industrial Ethernet.

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-2022-27640

The affected devices improperly handles excessive ARP broadcast requests.

This could allow an attacker to create a denial of service condition by performing ARP storming attacks, which can cause the device to reboot.

CVSS v3.1 Base Score	7.4
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-400: Uncontrolled Resource Consumption

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 (2022-05-10):	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.