SSA-516818: TCP Sequence Number Validation Vulnerability in the TCP/IP Stack of CP343-1 Devices

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: 8.7

SUMMARY

Affected products incorrectly validate TCP sequence numbers. This could allow an unauthenticated remote attacker to create a denial of service condition by injecting spoofed TCP RST packets.

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

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC CP 343-1 (6GK7343-1EX30-0XE0): All versions affected by all CVEs	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIMATIC CP 343-1 Lean (6GK7343-1CX10-0XE0): All versions affected by all CVEs	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS NET CP 343-1 (6AG1343-1EX30-7XE0): All versions affected by all CVEs	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SIPLUS NET CP 343-1 Lean (6AG1343-1CX10-2XE0): 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:

- Apply network segmentation and Defense-in-Depth practices to reduce likelihood of a threat actor to be able to reach a potentially vulnerable device

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 CP 343-1 are communication processors (CP) designed to enable Ethernet communication for SIMATIC S7-300 CPUs.

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 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-2023-51440

Affected products incorrectly validate TCP sequence numbers. This could allow an unauthenticated remote attacker to create a denial of service condition by injecting spoofed TCP RST packets.

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:T/RC:C
CVSS v4.0 Base Score	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N
CWE	CWE-940: Improper Verification of Source of a Communication Channel

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