SSA-549234: Denial-of-Service Vulnerability in SIMATIC NET CP Modules

Publication Date:	2021-09-14
Last Update:	2021-12-14
Current Version:	V1.1
CVSS v3.1 Base Score:	7.5

SUMMARY

A denial of service vulnerability was identified in different types of Communication Processors. An attacker could exploit this vulnerability causing the device to become un-operational until the device is restarted.

Siemens is preparing updates and recommends specific countermeasures for products where updates are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC CP 343-1 (incl. SIPLUS variants): All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SIMATIC CP 343-1 Advanced (incl. SIPLUS variants): All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SIMATIC CP 343-1 ERPC: All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SIMATIC CP 343-1 Lean (incl. SIPLUS variants): All versions	Currently no remediation is planned See recommendations from section Workarounds and Mitigations
SIMATIC CP 443-1 (incl. SIPLUS variants): All versions	Currently no remediation is available See recommendations from section Workarounds and Mitigations
SIMATIC CP 443-1 Advanced (incl. SIPLUS variants): All versions	Currently no remediation is available 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:

- Limit access to port 102/tcp to trusted users and systems 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

Communication Processor (CP) modules of families SIMATIC CP 343-1 and CP 443-1 have been designed to enable SIMATIC S7-300/S7-400 CPUs for Ethernet communication.

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-2021-33737

Sending a specially crafted packet to port 102/tcp of an affected device could cause a denial of service condition. A restart is needed to restore normal operations.

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:U/RC:C
CWE	CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Michael Messner from Siemens Energy for reporting the vulnerability

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
V1.1 (2021-12-14):	Specifically added that SIMATIC CP 343-1 devices do not have any fix planned

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.