SSA-280603: Denial of Service Vulnerability in SINUMERIK ONE and SINUMERIK MC

Publication Date: 2023-12-12
Last Update: 2024-09-10
Current Version: V1.1
CVSS v3.1 Base Score: 7.5

SUMMARY

A vulnerability has been identified in the integrated S7-1500 CPU of SINUMERIK ONE and SINUMERIK MC products that could allow an attacker to cause a denial of service condition. In order to exploit the vulnerability, an attacker must have access to the affected devices on port 102/tcp.

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

Note: The affected integrated S7-1500 CPUs and related products are advised in [1].

[1] https://cert-portal.siemens.com/productcert/html/ssa-592380.html

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SINUMERIK MC: All versions < V1.24 affected by CVE-2023-46156	Update to V1.24 or later version Updated software version can be obtained from Siemens customer support or a local partner. See further recommendations from section Workarounds and Mitigations
SINUMERIK ONE: All versions < V6.24 affected by CVE-2023-46156	Update to V6.24 or later version Updated software version can be obtained from Siemens customer support or a local partner. See further 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:

- Expose port 102/tcp of the integrated S7-1500 CPU only to trusted network environments

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

SINUMERIK MC is a CNC system for customized machine solutions.

SINUMERIK ONE is a digital-native CNC system with an integrated SIMATIC S7-1500 CPU for automation.

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-2023-46156

Affected devices improperly handle specially crafted packets sent to port 102/tcp. This could allow an attacker to create 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:O/RC:C
CWE	CWE-416: Use After Free

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Maurice Joren for reporting and coordinated disclosure
- Yu Cong for reporting and coordinated disclosure

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 (2023-12-12): Publication Date
V1.1 (2024-09-10): Added fix for SINUMERIK ONE and SINUMERIK MC

TERMS OF USE