SSA-118850: Denial of Service Vulnerability in the OPC UA Implementation in SINUMERIK ONE and SINUMERIK MC

Publication Date: 2023-12-12
Last Update: 2023-12-12
Current Version: V1.0
CVSS v3.1 Base Score: 7.5

SUMMARY

SINUMERIK ONE and SINUMERIK MC products are affected by a denial of service vulnerability in the OPC UA implementation of the integrated S7-1500 CPU. The vulnerability in the integrated S7-1500 CPU is documented in more detail in SSA-711309 [1].

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

[1] https://cert-portal.siemens.com/productcert/html/ssa-711309.html

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SINUMERIK MC: All versions < V1.22	Update to V1.22 or later version https://support.industry.siemens.com/cs/ww/en/view/109824227/ See further recommendations from section Workarounds and Mitigations
SINUMERIK ONE: All versions < V6.22	Update to V6.22 or later version https://support.industry.siemens.com/cs/ww/en/view/109824227/ 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 the OPC UA interface 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 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-2023-28831

The OPC UA implementations (ANSI C and C++) in affected products contain an integer overflow vulnerability that could cause the application to run into an infinite loop during certificate validation.

This could allow an unauthenticated remote attacker to create a denial of service condition by sending a specially crafted certificate.

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-190: Integer Overflow or Wraparound

ADDITIONAL INFORMATION

For more information regarding CVE-2023-28831 refer to the Siemens Security Advisory SSA-711309 (https://cert-portal.siemens.com/productcert/html/ssa-711309.html)

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

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.