SSA-568428: Weak Key Protection Vulnerability in SINUMERIK ONE and SINUMERIK MC

Publication Date: 2022-11-08
Last Update: 2023-02-14
Current Version: V1.1
CVSS v3.1 Base Score: 9.3

SUMMARY

SINUMERIK ONE and SINUMERIK MC products are affected by a weak key protection vulnerability in the integrated S7-1500 CPU. The weak key protection vulnerability in the integrated S7-1500 CPU is documented in more detail in SSA-568427 [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-568427.html

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SINUMERIK MC: All versions < V6.21	Update to V6.21 or later version SINUMERIK software can be obtained from your local Siemens account manager. See further recommendations from section Workarounds and Mitigations
SINUMERIK ONE: All versions < V6.21	Update to V6.21 or later version SINUMERIK software can be obtained from your local Siemens account manager. 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 communication between the S7-1500 CPU and the HMI of the affected products only to trusted network environments
- Protect access to the TIA Portal project and SINUMERIK NCU (including related memory cards) from unauthorized actors

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-2022-38465

Affected products protect the built-in global private key in a way that cannot be considered sufficient any longer. The key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication.

This could allow attackers to discover the private key of a CPU product family by an offline attack against a single CPU of the family. Attackers could then use this knowledge to extract confidential configuration data from projects that are protected by that key or to perform attacks against legacy PG/PC and HMI communication.

CVSS v3.1 Base Score	9.3
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-522: Insufficiently Protected Credentials

ADDITIONAL INFORMATION

For more information regarding CVE-2022-38465 refer to the Siemens Security Advisory SSA-568427 (https://cert-portal.siemens.com/productcert/html/ssa-568427.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 (2022-11-08): Publication Date
V1.1 (2023-02-14): Added fix information for SINUMERIK MC and SINUMERIK ONE

TERMS OF USE