SSA-568427: Weak Key Protection Vulnerability in SIMATIC S7-1200 and S7-1500 CPU Families

Publication Date:	2022-10-11
Last Update:	2022-10-11
Current Version:	V1.0
CVSS v3.1 Base Score:	9.3

SUMMARY

SIMATIC S7-1200, S7-1500 CPUs and related 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.

Siemens recommends to update both the affected products as well as the corresponding TIA Portal project to the latest versions. TIA Portal V17 and related CPU firmware versions introduced protection of confidential configuration data based on individual passwords per device and TLS-protected PG/PC and HMI communication.

Additional details can be found in the related Siemens security bulletin SSB-898115 (https://cert-portal.siemens.com/productcert/html/ssb-898115.html).

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC Drive Controller family: All versions < V2.9.2	Update to V2.9.2 or later version, migrate project in TIA Portal to this version and redeploy. Within the project, configure the CPU to “Only allow secure PG/PC and HMI communication” https://support.industry.siemens.com/cs/ww/en/view/109773914/ See further recommendations from section Workarounds and Mitigations
SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants): All versions < V21.9	Update to V21.9 or later version, migrate project in TIA Portal to this version and redeploy. Within the project, configure the CPU to “Only allow secure PG/PC and HMI communication” https://support.industry.siemens.com/cs/ww/en/view/109759122/ See further recommendations from section Workarounds and Mitigations
SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants): All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations

SIMATIC S7-1200 CPU family (incl. SIPLUS variants): All versions < V4.5.0	Update to V4.5.0 or later version, migrate project in TIA Portal to this version and redeploy. Within the project, configure the CPU to "Only allow secure PG/PC and HMI communication" https://support.industry.siemens.com/cs/ww/en/view/109793280/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants): All versions < V2.9.2	Update to V2.9.2 or later version, migrate project in TIA Portal to this version and redeploy. Within the project, configure the CPU to "Only allow secure PG/PC and HMI communication" https://support.industry.siemens.com/cs/ww/en/view/109478459/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-1500 Software Controller: All versions < V21.9	Update to V21.9 or later version, migrate project in TIA Portal to this version and redeploy. Within the project, configure the CPU to "Only allow secure PG/PC and HMI communication" https://support.industry.siemens.com/cs/ww/en/view/109478528/ See further recommendations from section Workarounds and Mitigations
SIMATIC S7-PLCSIM Advanced: All versions < V4.0	Update to V4.0 or later version, migrate project in TIA Portal to the corresponding version and redeploy. Within the project, configure the CPU to "Only allow secure PG/PC and HMI communication" https://support.industry.siemens.com/cs/ww/en/view/109795016/ 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:

- Use legacy (i.e., not TLS-based) PG/PC and HMI communication only in trusted network environments
- Protect access to the TIA Portal project and CPU (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

SIMATIC Drive Controllers have been designed for the automation of production machines, combining the functionality of a SIMATIC S7-1500 CPU and a SINAMICS S120 drive control.

SIMATIC ET 200SP Open Controller is a PC-based version of the SIMATIC S7-1500 Controller including optional visualization in combination with central I/Os in a compact device.

SIMATIC S7-1200 CPU products have been designed for discrete and continuous control in industrial environments such as manufacturing, food and beverages, and chemical industries worldwide.

SIMATIC S7-1500 CPU products have been designed for discrete and continuous control in industrial environments such as manufacturing, food and beverages, and chemical industries worldwide.

SIMATIC S7-1500 Software Controller is a SIMATIC software controller for PC-based automation solutions.

SIMATIC S7-PLCSIM Advanced simulates S7-1200, S7-1500 and a few other PLC derivatives. Includes full network access to simulate the PLCs, even in virtualized environments.

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-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

ACKNOWLEDGMENTS

Siemens thanks the following party for its efforts:

- Tal Keren from Claroty for coordinated disclosure

ADDITIONAL INFORMATION

Additional details can be found in the related Siemens security bulletin SSB-898115 (https://cert-portal.siemens.com/productcert/html/ssb-898115.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 (2022-10-11):	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.