SSB-898115: Remarks Regarding 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

Summary

Siemens publishes this bulletin to provide additional information about SSA-568427: “Weak Key Protection Vulnerability in SIMATIC S7-1200 and S7-1500 CPU Families” [0].

Fixes for affected products are available. Siemens recommends updating both the affected PLCs and the TIA Portal project as stated in SSA-568427. If an update is not possible, Siemens recommends following the workarounds and mitigations described in SSA-568427.

History

In early 2013 Siemens introduced standards-based asymmetric cryptography into the integrated security architecture with TIA Portal V12 and SIMATIC S7-1200 and S7-1500 CPU families to satisfy the following security goals:

- Integrity protection and confidentiality for the devices and customer programs
- Integrity protection and confidentiality for the communication between devices in the industrial control system

At the time of the development of the architecture, practical solutions for dynamic key management and key distribution did not exist for industrial control systems. The additional operational effort that key management solutions impose for integrators and customers was not justifiable.
Because of these restrictions and the residual risk of the security threat modeling for the architecture, Siemens decided to go with an approach based on fixed key material. As both technology and threat landscape evolved significantly in the past years, this decision needs to be revised and adapted.

Problem Description

As stated in SSA-568427 [0], SIMATIC S7-1200 and S7-1500 PLCs use a built-in global private key which cannot be considered anymore as sufficiently protected. This key is used for the legacy protection of confidential configuration data and the legacy PG/PC and HMI communication. An offline attack against a single PLC allows sophisticated attackers to discover the global private key and then use this knowledge to perform two types of attack:

Attack 1: Extract confidential configuration data

With access to the TIA Portal project or the project stored on the PLC (including memory card), an attacker could extract confidential configuration data. These data are cryptographic keys and passwords which are used for certificate-based communication like https, OPC UA, or secure Open User Communication and for the protection of the PLC (access level passwords).

Attack 2: Attacks against legacy PG/PC and HMI communication

With Man-in-the-Middle attacks, attacker could read, modify, and selectively forward data between the PLC and its connected HMIs and Engineering-Stations.

Solution

Since the release of TIA Portal V17 and related CPU FW versions, the protection of confidential configuration data is based on an individual password per device and the PG/PC and HMI communication is protected by TLS V1.3. With these security improvements PLCs are not vulnerable to attacks using the global private key.

Siemens is not aware of related cybersecurity incidents but considers the likelihood of malicious actors misusing the global private key as increasing and strongly recommends to follow the remediations described in SSA-568427 and to update both, the TIA Portal project to V17 and CPU to related firmware version.

CPU firmware versions which are recommended to update to:

- SIMATIC Drive Controller family >= V2.9.2
- SIMATIC ET 200SP Open Controller 2 >= V21.9
- SIMATIC S7-1200 CPU family >= V4.5.0
- SIMATIC S7-1500 CPU family >= V2.9.2
- SIMATIC S7-1500 SW Controller >= V21.9
- PLCSIM Advanced >= V4.0

It is important to note that an update of the firmware on the device is not sufficient. In addition, the hardware configuration in the TIA Portal project (V17 or later) must also be updated to the corresponding CPU version and downloaded to the PLC.

By default, PLCs configured with TIA Portal V17 and its related CPU version have all necessary security improvements enabled:

- Users are asked to add an individual password for the protection of the confidential PLC configuration data. This password is used for encryption of keys for certificate-based protocols and other data worth protecting. It is possible to proceed without setting the password if you have implemented measures to prevent unauthorized access to the TIA Portal project and the CPU.
- To protect the communication between PLC and its HMIs or Engineering-Stations, by default only TLS-based communication (secure PG/PC and HMI communication) is allowed. To support compatibility with HMIs and Engineering-Stations with versions below TIA Portal V17, customers can explicitly activate the legacy PG/PC and HMI communication in the TIA Portal configuration of the PLC. It is important to know that, if the legacy PG/PC and HMI communication is enabled in the configuration, the security level will be reduced significantly: attackers with access to the network and knowledge of the global private key could attack the PLC (see attack 2).

Workarounds and Mitigations

Siemens strongly recommends updating affected devices as stated in SSA-568427 [0]. Customers who are not able to update should implement the following workarounds and mitigations to minimize the risk of attacks:

- Use the legacy PG/PC and HMI communication only in trusted network environments.
  - Projects before TIA Portal V17:
    The legacy PG/PC and HMI communication is the standard communication. The secure communication based on TLS is not supported for projects before TIA Portal V17. Network access to PLC and HMIs or Engineering-Stations must be restricted to authorized users only.
  - Projects with TIA Portal V17:
    Since TIA Portal V17, legacy PG/PC and HMI communication is disabled by default but can be enabled in the PLC configuration. Legacy PG/PC and HMI communication should be enabled only if it is not possible to update HMIs and Engineering-Stations to TIA Portal V17 and if network access to PLC and HMIs or Engineering-Stations can be restricted to authorized users only.
- Protect access to the TIA Portal project and CPU from unauthorized actors.
  The confidential configuration data are part of the TIA Portal Project and the PLC configuration stored in the PLC (including memory card).

As a general security measure, Siemens strongly recommends protecting network access to devices with appropriate mechanisms. To operate the devices in a protected IT environment, Siemens recommends configuring the environment according to Siemens' operational guidelines for Industrial Security [1], and to follow the recommendations in the product manuals.
To mitigate the risk of attacks described in this bulletin, apply "defense in depth" as outlined on pages 12ff of the guidelines [1].

Acknowledgements

Siemens would like to thank Team82 of Claroty for reporting this issue, the related research effort and the close collaboration during the coordinated disclosure.

References

[0] https://cert-portal.siemens.com/productcert/html/ssa-568427.html

[1] https://www.siemens.com/cert/operational-guidelines-industrial-security

HISTORY DATA

V1.0 (2022-10-11): Publication Date

TERMS OF USE