SSA-240718: Insecure storage of HTTPS CA certificate in SIMATIC S7-1200 V2.x

Publication Date: 2012-09-13
Last Update: 2020-02-10
Current Version: V1.1
CVSS v3.1 Base Score: 6.8

SUMMARY

For the convenience of the customer, a Certificate Authority (CA) for HTTPS connections is installed on the Siemens SIMATIC S7-1200 PLC. The user has the option to trust this CA which if selected installs the certificate into the browser's certificate store. Once the user completes this step, the browser will trust any other S7-1200 V2.x PLC on the network.

A researcher has demonstrated the ability to obtain the private key of the S7-1200 CA ("SIMATIC CONTROLLER"). With this private key, an attacker is able to create his own certificate. Using this forged certificate, it is possible to spoof any SSL server certificate and conduct man-in-the-middle attacks on a user's browser that is currently trusting this CA.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC S7-1200 CPU family (incl. SIPLUS variants): V2.x	See 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:

- Siemens strongly recommends the user uninstall the CA keys from the browser's certificate store. Once this is performed, warning messages will occur when attempting to connect to an S7-1200 PLC. The user can manually confirm the identity of the PLC and its certificate and accept it via the browser. This has to be done once for each S7-1200 PLC on the network.

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

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

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 SVE-2012-0003

The private key for the CA "SIMATIC CONTROLLER" in the S7-1200 V2.x has been compromised. This could allow an attacker to perform man-in-the-middle attacks or to deploy malicious but trusted web sites.

CVSS v3.1 Base Score	6.8
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C
CWE	CWE-321: Use of Hard-coded Cryptographic Key

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Dmitry Sklyarov from Positive Technologies for coordinated disclosure
- Industrial Control System Cyber Emergency Response Team (ICS-CERT) for coordination efforts
- Artem Zinenko from Kaspersky for pointing out that SIPLUS should also be mentioned

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 (2012-09-13): Publication Date
V1.1 (2020-02-10): SIPLUS devices now explicitly mentioned in the list of affected products

TERMS OF USE