SSA-625789: Security Vulnerabilities in Siemens SIMATIC S7-1200 CPU

Publication Date: 2011-06-10
Last Update: 2020-02-10
Current Version: V2.2
CVSS v3.1 Base Score: 7.5

SUMMARY

Security experts have examined the SIMATIC S7-1200 Programmable Logic Controller (PLC). This research has revealed some weaknesses in the SIMATIC S71200 CPU communication and authentication functions. Once the automation network is compromised it is possible to demonstrate the following weaknesses using a remote exploit: - Trigger CPU functions by record and playback of legitimate network communication - Place CPU in stop/defect state by causing a communications error A remote exploit is a type of attack that can be launched from one computer against another computer across a network. For example, a PC with access to the automation network could be used to launch a remote exploit against a PLC.

The weaknesses are closed with a firmware update V 2.0.3. For the second weakness (communications error), a temporary work-around is also available: if the Web server on the S7-1200 is disabled, the weakness cannot be exploited.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC S7-1200 CPU family (incl. SIPLUS variants): All versions < V2.0.2	Update to V2.0.3 http://support.automation.siemens.com/WW/view/en/41886031/130000
SIMATIC S7-1200 CPU family (incl. SIPLUS variants): All versions < V2.0.3 only affected by SVE-2011-0001	Update to V2.0.3 http://support.automation.siemens.com/WW/view/en/41886031/130000

WORKAROUNDS AND MITIGATIONS

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- Disable the web server on the S7-1200 if possible

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-2011-0001

Prior to applying the latest firmware update (V 2.0.3) it was possible to place the controller in the stop/defect state by causing a communications error (e.g., by running a network scan sending malformed HTTP traffic at high rate). Thus a communications error occurred in the Web server interface of the S7-1200 causing the controller to enter the stop/defect state. In automation applications, the stop/defect state is a defined state in which the external process (e.g. the machine) is stopped, comparable to a power loss.

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-20: Improper Input Validation

Vulnerability SVE-2011-0002

Prior to applying the latest firmware update (V 2.0.3) it was possible to record communication between the engineering software and the controller using available open source tools and to replay the communication to the controller at a later time. This made it possible to execute any previously recorded commands issued by the engineering software to the PLC at a later time (e.g. set controller to STOP). This was true whether or not the controller had a password configured.

CVSS v3.1 Base Score	6.8
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-294: Authentication Bypass by Capture-replay

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Dillon Beresford from NSS Labs for his investigations

- 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 (2011-06-10):	Publication Date
V2.0 (2011-07-05):	Modification of CVSS scoring, solution and version information
V2.1 (2011-09-12):	Update of solution section by removing mentioning of air gap
V2.2 (2020-02-10):	SIPLUS devices now explicitly mentioned in the list of affected products

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.