SSA-603476: Web Vulnerabilities in SIMATIC NET CP 343-1/CP 443-1 Modules and SIMATIC S7-300/S7-400 CPUs

Publication Date: 2016-11-21
Last Update: 2023-04-11
Current Version: V1.4
CVSS v3.1 Base Score: 6.3

SUMMARY

SIMATIC CP 343-1 Advanced/CP-443-1 Advanced devices and SIMATIC S7-300/S7-400 CPUs are affected by two vulnerabilities. One of the vulnerabilities could allow remote attackers to perform operations as an authenticated user under certain conditions.

Siemens has released updates for several affected products and recommends to update to the latest versions. Siemens recommends specific countermeasures for products where updates are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC CP 343-1 Advanced (incl. SIPLUS variants): All versions < V3.0.53	Update to V3.0.53 or any later version https://support.industry.siemens.com/cs/ww/en/view/109742236 See further recommendations from section Workarounds and Mitigations
SIMATIC CP 443-1 Advanced (incl. SIPLUS variants): All versions < V3.2.17	Update to V3.2.17 or any later version https://support.industry.siemens.com/cs/ww/en/view/109745388 See further recommendations from section Workarounds and Mitigations
SIMATIC S7-300 CPU family (incl. related ET200 CPUs and SIPLUS variants): All versions < V3.X.18	Update to V3.X.18 or later version https://support.industry.siemens.com/cs/ww/en/ps/13752/dl See recommendations from section Workarounds and Mitigations
SIMATIC S7-400 PN/DP CPU family (incl. SIPLUS variants): All versions	Currently no fix is planned 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:

- Deactivate the webserver if not required, and if deactivation is supported by the product

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 CP 343-1 and CP 443-1 are communication processors (CP) designed to enable Ethernet communication for SIMATIC S7-300/S7-400 CPUs.

SIMATIC S7-300 controllers have been designed for discrete and continuous control in industrial environments such as manufacturing, food and beverages, and chemical industries worldwide.

SIMATIC S7-400 controllers 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 CVE-2016-8672

The integrated web server delivers cookies without the “secure” flag. Modern browsers interpreting the flag would mitigate potential data leakage in case of clear text transmission.

CVSS v3.1 Base Score	4.0
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-614: Sensitive Cookie in HTTPS Session Without 'Secure' Attribute

Vulnerability CVE-2016-8673

The integrated web server at port 80/TCP or port 443/TCP of the affected devices could allow remote attackers to perform actions with the permissions of an authenticated user, provided the targeted user has an active session and is induced to trigger the malicious request.

CVSS v3.1 Base Score	6.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C
CWE	CWE-345: Insufficient Verification of Data Authenticity

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Artem Zinenko from Kaspersky Lab for reporting inaccuracies in version 1.1 of this advisory and for pointing out that SIPLUS should also be mentioned
- Inverse Path auditors in collaboration with Airbus ICT Industrial Security team for coordinated disclosure of the vulnerabilities

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 (2016-11-21):	Publication Date
V1.1 (2017-03-16):	Added update information for SIMATIC CP 443-1 Advanced
V1.2 (2019-11-12):	Corrected affected products from S7-400 CPUs to S7-400 PN/DP incl. F as not all S7-400 CPUs are affected
V1.3 (2019-12-10):	SIPLUS devices now explicitly mentioned in the list of affected products
V1.4 (2023-04-11):	Added fix for SIMATIC S7-300 CPU familiy, no fix planned for SIMATIC S7-400 CPU familiy

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.