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

Publication Date 2016-11-21
Last Update 2017-03-16
Current Version V1.1
CVSS v3.0 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 SIMATIC CP 343-1 Advanced and SIMATIC CP 443-1 Advanced devices. Siemens recommends applying specific countermeasures for the remaining affected products. Siemens will update this advisory when new information becomes available.

AFFECTED PRODUCTS

- SIMATIC CP 343-1 Advanced: All versions < V3.0.53
- SIMATIC CP 443-1 Advanced: All versions < V3.2.17
- SIMATIC S7-300 CPU family: All firmware versions
- SIMATIC S7-400 CPU family: All firmware versions

DESCRIPTION

Communication Processor (CP) modules SIMATIC CP 343-1 Advanced and CP 443-1 Advanced have been designed to enable SIMATIC S7-300/S7-400 CPUs for Ethernet communication.

Siemens SIMATIC S7-300 CPU and S7-400 CPU families have been designed for discrete and continuous control in industrial environments such as manufacturing, food and beverages, and chemical industries worldwide.

Detailed information about the vulnerabilities is provided below.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.0 (CVSS v3.0) (http://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.

Vulnerability 1 (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 Base Score 6.3
CVSS Vector CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L/E:P/RL:O/RC:C

Vulnerability 2 (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 Base Score 4.0
CVSS Vector CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:N/A:N/E:P/RL:O/RC:C

Mitigating Factors

Siemens recommends operating SIMATIC S7-300/S7-400 CPUs only within trusted networks [3].

SOLUTION

Siemens provides firmware version V3.0.53 [1] for SIMATIC CP 343-1 Advanced devices which fixes the vulnerabilities and recommends customers update to the new version.

Siemens provides firmware version V3.2.17 [2] for SIMATIC CP 443-1 Advanced devices which fixes the vulnerabilities and recommends customers update to the new version.

For SIMATIC S7-300/S7-400 CPUs, Siemens recommends the following mitigations:

- Apply cell protection concept [3]
- Use VPN for protecting network communication between cells
- Apply Defense-in-Depth [3]

Siemens will update this Advisory when new information becomes available.

As a general security measure Siemens strongly recommends to protect network access to SIMATIC S7-300/S7-400 CPUs and to the web interface of SIMATIC CP 343-1 Advanced and CP 443-1 Advanced devices with appropriate mechanisms. It is advised to configure the environment according to our operational guidelines [3] in order to run the devices in a protected environment.

ACKNOWLEDGEMENTS

Siemens thanks Inverse Path auditors in collaboration with Airbus ICT Industrial Security team for coordinated disclosure of the vulnerabilities.

ADDITIONAL RESOURCES

[1] Firmware version V3.0.53 for SIMATIC CP 343-1 Advanced can be obtained here: https://support.industry.siemens.com/cs/ww/en/view/109742236

[2] Firmware version V3.2.17 for SIMATIC CP 443-1 Advanced can be obtained here: https://support.industry.siemens.com/cs/ww/en/view/109745388

[3] An overview of the operational guidelines for Industrial Security (with the cell protection concept): https://www.siemens.com/cert/operational-guidelines-industrial-security

[4] Information about Industrial Security by Siemens: https://www.siemens.com/industrialsecurity

[5] For further inquiries on 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

DISCLAIMER