SSA-731239: Vulnerabilities in SIMATIC S7-300 and S7-400 CPUs

Publication Date 2016-12-09
Last Update 2017-07-21
Current Version V1.2
CVSS v3.0 Base Score 7.5

SUMMARY

Two vulnerabilities have been identified in SIMATIC S7-300 and S7-400 CPU families. One vulnerability could lead to a Denial-of-Service, the other vulnerability could result in credential disclosure.

Siemens recommends specific mitigations. Siemens will update this advisory when new information becomes available.

AFFECTED PRODUCTS

- SIMATIC S7-300 CPU family: All versions
- SIMATIC S7-400 CPU family: All versions

DESCRIPTION

Products of the Siemens SIMATIC S7-300 and S7-400 CPU family 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 assessed by the customer to accomplish final scoring.

Vulnerability 1 (CVE-2016-9158)

Specially crafted packets sent to port 80/tcp could cause the affected devices to go into defect mode. A cold restart is required to recover the system. This vulnerability affects all SIMATIC S7-300 PN CPUs, and all SIMATIC S7-400 PN V6 and V7 CPUs.

CVSS Base Score 7.5
CVSS Vector CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:T/RC:C

Vulnerability 2 (CVE-2016-9159)

An attacker with network access to port 102/tcp (ISO-TSAP) or via Profibus could obtain credentials from the PLC if protection-level 2 is configured on the affected devices. This vulnerability affects all listed affected products.

CVSS Base Score 7.5
Vector CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:T/RC:C

Mitigating Factors

The attacker must have network access to the affected devices.

Vulnerability 1 only applies if the web server is manually activated in the project configuration.

Vulnerability 2 only applies if protection-level 2 is activated in the project configuration.

Siemens recommends operating the devices only within trusted networks [3].

SOLUTION

Siemens provides firmware version V3.X.14 [1] for S7-300 CPUs that resolves vulnerability 1 (CVE-2016-9158).

Siemens recommends applying firmware version V8.2 [2] to S7-CPU 410 CPUs, activating Field Interface Security in PCS 7 V9.0, and using a CP 443-1 Adv. to communicate with ES/OS in order to mitigate vulnerability 2.

For the remaining vulnerabilities or products, Siemens recommends the following mitigations:

- Deactivate the web server (vulnerability 1)
- Apply protection-level 3 (Read/Write protection for vulnerability 2)
- Apply cell protection concept [3]
- Apply Defense-in-Depth concept [4]
- Use VPN for protecting network communication between cells

Siemens will update this advisory when new information becomes available.

As a general security measure Siemens strongly recommends to keep the firmware up-to-date and to protect network access to S7-300 and S7-400 CPUs with appropriate mechanisms. In addition, it is advised to configure the environment according to our operational guidelines [3] in order to run the devices in a protected IT environment.

ACKNOWLEDGEMENTS

Siemens thanks the following parties for their support and efforts:

- Zhu WenZhe from Beijing Acorn Network Technology Co., Ltd. for coordinated disclosure of the vulnerabilities.
- Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) for reporting the vulnerability and coordination efforts.

ADDITIONAL RESOURCES

[1] Firmware version V3.X.14 for S7-300 CPUs can be obtained from:
https://support.industry.siemens.com/cs/ww/en/ps/13752/dl

[2] Firmware version V8.2 for SIMATIC S7-410 can be obtained from:
https://support.industry.siemens.com/cs/ww/en/view/109476571

[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] Further information about Defense-in-Depth:
http://www.industry.siemens.com/topics/global/en/industrial-security/concept/Pages/defense-in-depth.aspx

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

[6] 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 (2016-12-09):	Publication Date
V1.1 (2017-05-08):	Added fix information for CVE-2016-9158 in S7-300 CPU family; Clarified that vulnerability CVE-2016-9159 also affects Profibus
V1.2 (2017-07-21):	Added mitigation for vulnerability 2 in S7-CPU 410.

DISCLAIMER

See: https://www.siemens.com/terms_of_use