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

Publication Date: 2016-12-09
Last Update: 2020-03-10
Current Version: V1.6
CVSS v3.1 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 AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC S7-300 CPU family (incl. related ET200 CPUs and SIPLUS variants): All versions	Update to V3.X.14 to mitigate the first vulnerability (CVE-2016-9158), and follow recommendations from section Workaround and Mitigations for the second vulnerability (CVE-2016-9159). https://support.industry.siemens.com/cs/ww/en/ps/13752/dl
SIMATIC S7-400 PN/DP V6 and below CPU family (incl. SIPLUS variants): All versions	Update to V6.0.6 to mitigate the first vulnerability (CVE-2016-9158), and follow recommendations from section Workaround and Mitigations for the second vulnerability (CVE-2016-9159). https://support.industry.siemens.com/cs/de/en/view/109474874
SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants): All versions	Update to V7.0.2 to mitigate the first vulnerability (CVE-2016-9158), and follow recommendations from section Workaround and Mitigations for the second vulnerability (CVE-2016-9159). https://support.industry.siemens.com/cs/ww/en/view/109752685
SIMATIC S7-410 V8 CPU family (incl. SIPLUS variants): All versions only affected by CVE-2016-9159	Update to V8.2 and follow recommendations from section Workarounds and Mitigations. https://support.industry.siemens.com/cs/ww/en/view/109476571

WORKAROUNDS AND MITIGATIONS

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

- Apply protection-level 3 (Read/Write protection for CVE-2016-9159)
- Apply cell protection concept: https://www.siemens.com/cert/operational-guidelines-industrial-security
- Apply Defense-in-Depth concept: https://www.siemens.com/industrialsecurity

- For SIMATIC S7-CPU 410 CPUs: Activate Field Interface Security in PCS 7 V9.0, and use a CP 443-1 Adv. to communicate with ES/OS in order to mitigate vulnerability 2 (CVE-2016-9159).

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

Products in the SIMATIC S7-400 CPU family have been designed for process control in industrial environments. They are used worldwide, e.g. in the automotive industry, mechanical equipment manufacture, warehousing systems, building engineering, steel industry, power generation and distribution, pharmaceuticals, food and beverages industry, or chemical industry.

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-2016-9158

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.

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:T/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability 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.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:T/RC:C
CWE	CWE-200: Information Exposure

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Zhu WenZhe from Beijing Acorn Network Technology Co., Ltd. for coordinated disclosure of the vulnerabilities
- Industrial Control System Cyber Emergency Response Team (ICS-CERT) for reporting the vulnerability and 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 (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 CVE-2016-9159 in S7-CPU 410
V1.3 (2017-11-23):	Added update information for SIMATIC S7-400 V6PN
V1.4 (2018-01-24):	New advisory format; Added update information for SIMATIC S7-400 V7
V1.5 (2020-02-10):	SIPLUS devices now explicitly mentioned in the list of affected products
V1.6 (2020-03-10):	Updated vulnerability description to not explicitly mention affected products

TERMS OF USE