

SSA-914382: Denial-of-Service Vulnerability in SIMATIC S7-400

Publication Date: 2018-05-15
Last Update: 2018-09-11
Current Version: V1.1
CVSS v3.0 Base Score: 7.5

SUMMARY

SIMATIC S7-400 CPUs are affected by a security vulnerability which could lead to a Denial-of-Service condition of the PLC if specially crafted packets are received and processed.

The affected SIMATIC S7-400 CPU hardware versions are in the product cancellation phase or already phased-out. Siemens recommends customers either upgrading to a new version or implementing specific countermeasures.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC S7-400 (incl. F) CPU hardware version 4.0 and below: All versions	See recommendations from section Workarounds and Mitigations or upgrade to hardware version 5.0 or newer https://support.industry.siemens.com/cs/ww/en/view/109483507
SIMATIC S7-400 (incl. F) CPU hardware version 5.0: All firmware versions < V5.2	Update to firmware version 5.2 or newer https://support.industry.siemens.com/cs/ww/en/view/109474827
SIMATIC S7-400H CPU hardware version 4.5 and below: All versions	See recommendations from section Workarounds and Mitigations or upgrade to hardware version 6.0 or newer https://support.industry.siemens.com/cs/ww/en/view/75407031

WORKAROUNDS AND MITIGATIONS

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

- Apply cell protection concept: <https://www.siemens.com/cert/operational-guidelines-industrial-security>.
- Use VPN for protecting network communication between cells.
- Apply Defense-in-Depth: <https://www.siemens.com/cert/operational-guidelines-industrial-security>.

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 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.

VULNERABILITY CLASSIFICATION

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

Vulnerability CVE-2018-4850

The affected CPUs improperly validate S7 communication packets which could cause a Denial-of-Service condition of the CPU. The CPU will remain in DEFECT mode until manual restart.

Successful exploitation requires an attacker to be able to send a specially crafted S7 communication packet to a communication interface of the CPU. This includes Ethernet, PROFIBUS, and Multi Point Interfaces (MPI). No user interaction or privileges are required to exploit the security vulnerability. The vulnerability could allow causing a Denial-of-Service condition of the core functionality of the CPU, compromising the availability of the system.

At the time of advisory publication no public exploitation of this security vulnerability was known. Siemens confirms the security vulnerability and provides mitigations to resolve the security issue.

CVSS v3.0 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:O/RC:C

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 (2018-05-15):	Publication Date
V1.1 (2018-09-11):	Added hint to Workarounds section

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.