

SSA-584286: Denial-of-Service Vulnerability in SIMATIC S7-1200 CPU and SIMATIC S7-1500 CPU

Publication Date: 2018-11-13
Last Update: 2018-11-13
Current Version: V1.0
CVSS v3.0 Base Score: 5.3

SUMMARY

A vulnerability was identified in SIMATIC S7-1200 and S7-1500 CPUs that could allow an attacker to cause a denial-of-service condition preventing HMI or engineering access to the PLC over port 102/tcp.

Siemens has released an update for the S7-1500 product and recommends that customers update to the new version. Siemens is preparing a further update for the S7-1200 product and recommends specific workarounds and mitigations until patches are available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC S7-1200: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC S7-1500: All Versions < V2.6	Update to V2.6 https://support.industry.siemens.com/cs/de/en/view/109478459

WORKAROUNDS AND MITIGATIONS

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

- Protect network access to port 102/tcp of affected devices
- Apply cell-protection concept
- Apply defense-in-depth

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 SIMATIC S7-1200 CPU family have been designed for discrete and continuous control in industrial environments such as manufacturing, food and beverages, and chemical industries worldwide.

Products of the SIMATIC S7-1500 CPU family have been designed for discrete and continuous control in industrial environments such as manufacturing, food and beverages, and chemical industries worldwide.

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-2018-13815

An attacker could exhaust the available connection pool of an affected device by opening a sufficient number of connections to the device.

Successful exploitation requires an attacker to be able to send packets to port 102/tcp of the affected device. No user interaction and no user privileges are required to exploit the vulnerability. The vulnerability, if exploited, could cause a Denial-of-Service condition impacting the availability of the system.

At the time of advisory publication no public exploitation of this vulnerability was known.

CVSS v3.0 Base Score	5.3
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Younes Dragoni from Nozomi Networks for coordinated disclosure
- Industrial Control System Cyber Emergency Response Team (ICS-CERT) for coordination efforts

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 (2018-11-13): Publication Date

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.