SSA-347726: Denial-of-Service Vulnerability in SIMATIC S7-1500, SIMATIC S7-1500 Software Controller and SIMATIC ET 200SP Open Controller

Publication Date: 2018-10-09
Last Update: 2020-02-10
Current Version: V1.2
CVSS v3.1 Base Score: 5.3

SUMMARY

Versions of SIMATIC S7-1500, SIMATIC S7-1500 Software Controller and SIMATIC ET200SP Open Controller are affected by a denial-of-service vulnerability. An attacker with network access to the PLC can cause a Denial-of-Service condition on the network stack.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC ET 200SP Open Controller (incl. SIPLUS variants): All versions >= V2.0 and < V2.1.6	Update to V2.1.6 https://support.industry.siemens.com/cs/us/en/view/109759122
SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants): All versions >= V2.0 and < V2.5	Update to V2.5 or newer https://support.industry.siemens.com/cs/us/en/ps/13717/dl
SIMATIC S7-1500 Software Controller: All versions >= V2.0 and < V2.5	Update to V2.5 or newer https://support.industry.siemens.com/cs/us/en/view/109478528

WORKAROUNDS AND MITIGATIONS

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

- Restrict network access to 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 S7-1500 CPU family have been designed for discrete and continuous control in industrial environments such as manufacturing, food and beverages, and chemical industries worldwide.

SIMATIC S7-1500 Software Controller is a SIMATIC software controller for PC-based automation solutions.

The SIMATIC ET 200SP Open Controller is a PC-based version of the SIMATIC S7-1500 Controller including optional visualization in combination with central I/Os in a compact device.

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-2018-13805

An attacker can cause a denial-of-service condition on the network stack by sending a large number of specially crafted packets to the PLC. The PLC will lose its ability to communicate over the network.

This vulnerability could be exploited by an attacker with network access to the affected systems. Successful exploitation requires no privileges and no user interaction. An attacker could use this vulnerability to compromise availability of the network connectivity.

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

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C
CWE	CWE-400: Uncontrolled Resource Consumption ('Resource Exhaustion')

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Marcin Dudek, Jacek Gajewski, Kinga Staszkiewicz, Jakub Suchorab, and Joanna Walkiewicz from National Centre for Nuclear Research Poland for coordinated disclosure
- 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 (2018-10-09):	Publication Date
V1.1 (2019-02-12):	Added solution for SIMATIC ET 200 SP Open Controller, SIMATIC S7-1500 Software Controller
V1.2 (2020-02-10):	SIPLUS devices now explicitly mentioned in the list of affected products

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.