SSA-589181: Denial-Of-Service in SIMATIC S7-200 SMART CPU Family Devices

Publication Date: 2020-07-14
Last Update: 2020-07-14
Current Version: V1.0
CVSS v3.1 Base Score: 7.5

SUMMARY

The latest update for SIMATIC S7-200 SMART fixes a vulnerability that could allow an attacker to cause a permanent Denial-of-Service of an affected device by sending a large number of crafted packets.

Siemens has released an update for the SIMATIC S7-200 SMART CPU family and recommends that customers update to the latest version.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC S7-200 SMART CPU family: All versions >= V2.2 < V2.5.1	Update to V2.5.1 https://support.industry.siemens.com/cs/ww/en/view/109765009/

WORKAROUNDS AND MITIGATIONS

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

- Limit network access to device to trusted sources.

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

The S7-200 SMART series is a line of micro-programmable logic controllers that can control a variety of small automation applications.

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-2020-7584

Affected devices do not properly handle large numbers of new incomming connections and could crash under certain circumstances. An attacker may leverage this to cause a Denial-of-Service situation.

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:O/RC:C
CWE	CWE-400: Uncontrolled Resource Consumption

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Ezequiel Fernandez from Dreamlab Technologies for related disclosure

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 (2020-07-14): Publication Date

TERMS OF USE