SSA-818183: Denial-of-Service Vulnerability in S7-300 CPU

Publication Date 2016-06-08
Last Update 2016-06-08
Current Version V1.0
CVSSv3 Base Score 7.5

SUMMARY

Siemens has released a firmware update for the SIMATIC S7-300 CPU family which fixes a vulnerability that could allow remote attackers to perform a Denial-of-Service attack under certain conditions.

AFFECTED PRODUCTS

- SIMATIC S7-300 CPUs with Profinet support: All versions < V3.2.12
- SIMATIC S7-300 CPUs without Profinet support: All versions < V3.3.12

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.

Detailed information about the vulnerability is provided below.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3 (CVSSv3) (http://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 Description (CVE-2016-3949)

Specially crafted packets sent to port 102/tcp (ISO-TSAP) or via Profibus could cause the affected device to go into defect mode. A cold restart is required to recover the system.

CVSS 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

Mitigating Factors

- The attacker must have network access to the affected device.
- Protection-level 3 (Read/Write protection) mitigates the issue.
- Siemens recommends operating the devices only within trusted networks [2].

SOLUTION

Siemens has released SIMATIC S7-300 firmware version V3.2.12 and V3.3.12 [1] which fixes the vulnerability and recommends customers to update to the latest version.

As a general security measure Siemens strongly recommends to keep the firmware up-to-date and to protect network access to the S7-300 CPUs with appropriate mechanisms. It is advised to configure the environment according to our operational guidelines [2] in order to run the devices in a protected IT environment.

ACKNOWLEDGEMENTS

Siemens thanks the following for their support and efforts:

- Mate J. Csorba, DNV GL, Marine Cybernetics Services for coordinated disclosure of the vulnerability.
- Amund Sole, Norwegian University of Science and Technology for coordinated disclosure of the vulnerability.

ADDITIONAL RESOURCES

[1] The firmware update for SIMATIC S7-300 CPUs can be obtained here:
https://support.industry.siemens.com/cs/ww/en/ps/13752

[2] An overview of the operational guidelines for Industrial Security (with the cell protection concept):
https://www.siemens.com/cert/operational-guidelines-industrial-security

[3] Information about Industrial Security by Siemens:
https://www.siemens.com/industrialsecurity

[4] For further inquiries on vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:
https://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2016-06-08): Publication Date

DISCLAIMER