SSA-987029: Denial-of-Service Vulnerability in S7-300

Publication Date 2015-03-05
Last Update 2015-03-05
Current Version V1.0
CVSS Overall Score 6.3

Summary:

A vulnerability could allow attackers to perform a Denial-of-Service attack over the network without prior authentication against S7-300 CPUs under certain conditions.

Siemens recommends specific mitigations. Siemens will update this advisory when new information becomes available.

AFFECTED PRODUCTS

- SIMATIC S7-300 CPU family: All versions

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 CVSSv2 scoring system (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-2015-2177)

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 7.8
CVSS Temporal Score 6.3
CVSS Overall Score 6.3 (AV:N/AC:L/Au:N/C:N/I:N/A:C/E:POC/RL:TF/RC:C)

Mitigating factors

The attacker must have network access to the affected devices.

Protection-level 3 (Read/Write protection) mitigates the issue.

Siemens recommends operating the devices only within trusted networks [1].

SOLUTION

Siemens recommends the following mitigations:

- Apply protection-level 3 (Read/Write protection)
- Apply cell protection concept [1]
- Use VPN for protecting network communication between cells
- Apply Defense-in-Depth [2]

Siemens will update this advisory when new information becomes available.

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 [3] in order to run the devices in a protected IT environment.

ACKNOWLEDGEMENT

Siemens thanks Johannes Klick, Christian Pfahl, Martin Gebert, and Lucas Jacob from Freie Universität Berlin's work team SCADACS for coordinated disclosure of the vulnerability.

ADDITIONAL RESOURCES

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

[2] Further information about Defense-in-Depth:
http://www.industry.siemens.com/topics/global/en/industrial-security/concept/Pages/defense-in-depth.aspx

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

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

HISTORY DATA

V1.0 (2015-03-05): Publication Date

DISCLAIMER