SSA-508982: Denial-of-Service Vulnerability in SIMATIC S7-300 CPUs, SIMATIC TDC, and SINUMERIK Controller over Profinet

Publication Date: 2020-03-10
Last Update: 2020-07-14
Current Version: V1.1
CVSS v3.1 Base Score: 7.5

SUMMARY

The latest firmware update for the S7-300 CPUs fixes a vulnerability that could allow an unauthenticated attacker with network access to cause a denial-of-service condition. SINUMERIK 840D sl Controller, which contains a S7-300 CPU, is also affected, as well as SIMATIC TDC.

Siemens has released updates for several affected products and recommends that customers update to the latest version(s).

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC S7-300 CPU family (incl. related ET200 CPUs and SIPLUS variants): All versions < V3.X.17	Update to V3.X.17 https://support.industry.siemens.com/cs/ww/en/ps/13752/dl
SIMATIC TDC CP51M1: All versions < V1.1.8	Update to V1.1.8 https://support.industry.siemens.com/cs/ww/en/view/27049282
SIMATIC TDC CPU555: All versions < V1.1.1	Update to V1.1.1 https://support.industry.siemens.com/cs/ww/en/view/109740119
SINUMERIK 840D sl: All versions < V4.8.6	Update to V4.8.6 SINUMERIK software can be obtained from your local Siemens account manager.
SINUMERIK 840D sl: All versions < V4.94	Update to V4.94 SINUMERIK software can be obtained from your local Siemens account manager.

WORKAROUNDS AND MITIGATIONS

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

- Make sure that access to port 102/tcp is restricted e.g. with an external firewall.

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 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.

SINUMERIK CNC offers automation solutions for the shop floor, job shops and large serial production environments.

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.

SIMATIC TDC is a multiprocessor automation system for drive, control and technology tasks. The system is used particularly for large plants.

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-2019-18336

Specially crafted packets sent to port 102/tcp (Profinet) could cause the affected device to go into defect mode. A restart is required in order to recover the system.

Successful exploitation requires an attacker to have network access to port 102/tcp, with no authentication. No user interation is required.

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

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

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Peter Cheng from Elex Cybersecurity INC. for coordinated disclosure
- CNCERT/CC 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 (2020-03-10):	Publication Date
V1.1 (2020-07-14):	Added SIMATIC TDC CP51M1 and SIMATIC TDC CPU555 to the list of affected products. Added solution for SINUMERIK 840D sl.

TERMS OF USE