SSA-250618: Denial-of-Service Vulnerability in SIMATIC TDC CP51M1

Publication Date: 2019-09-10
Last Update: 2019-09-10
Current Version: V1.0
CVSS v3.0 Base Score: 7.5

SUMMARY

A vulnerability could allow an attacker to cause a Denial-of-Service condition on the UDP communication by sending a specially crafted UDP packet to the SIMATIC TDC CP51M1 module.

Siemens has released an update for SIMATIC TDC CP51M1 module and recommends that customers update to the new version.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC TDC CP51M1: All versions < V1.1.7	Update to V1.1.7 https://support.industry.siemens.com/cs/ww/en/view/27049282

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
- Restrict UDP communication to affected devices
- Do not use UDP communication in the user program if not needed
- Apply cell protection concept and implement 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

SIMATIC TDC is a multiprocessor automation system for drive, control and technology tasks. The system is used particularly for large plants. The CP51M1 module enables ethernet communication.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.0 (CVSS v3.0) (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.

Vulnerability CVE-2019-10937

An attacker with network access to the device could cause a Denial-of-Service condition by sending a specially crafted UDP packet. The vulnerability affects the UDP communication of the device.

The security vulnerability could be exploited without authentication. No user interaction is required to exploit this security vulnerability. Successful exploitation of the security vulnerability compromises availability of the targeted system.

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

CVSS v3.0 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

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 (2019-09-10): Publication Date

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.