SSA-256092: Multiple local Denial-of-Service Vulnerabilities in SIMATIC S7-PLCSIM V5.4

Publication Date: 2021-03-09
Last Update: 2021-03-09
Current Version: V1.0
CVSS v3.1 Base Score: 5.5

SUMMARY

Multiple vulnerabilities affecting SIMATIC S7-PLCSIM V5.4 could allow an attacker with local access to the system to craft special project files that may lead to denial-of-service attacks.

Siemens recommends specific workarounds and mitigations.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC S7-PLCSIM V5.4: All versions	See recommendations from section Workarounds and Mitigations

WORKAROUNDS AND MITIGATIONS

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

- Restrict access to project files on the engineering station to trusted users.
- Only use project files from 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

SIMATIC S7-PLCSIM V5.4 is a Windows application that simulates the execution of user programs for the SIMATIC S7-300 CPU, S7-400 CPU, and WinAC families of controllers.

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-2021-25673

An attacker with local access to the system could cause a Denial-of-Service condition in the application when it is used to open a specially crafted file. As a consequence, the application could enter an infinite loop, become unresponsive and must be restarted to restore the service.

CVSS v3.1 Base Score	5.5
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:W/RC:C
CWE	CWE-835: Loop with Unreachable Exit Condition (‘Infinite Loop’)

Vulnerability CVE-2021-25674

An attacker with local access to the system could cause a Denial-of-Service condition in the application when it is used to open a specially crafted file. As a consequence, a NULL pointer deference condition could cause the application to terminate unexpectedly and must be restarted to restore the service.

CVSS v3.1 Base Score	5.5
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:W/RC:C
CWE	CWE-476: NULL Pointer Dereference

Vulnerability CVE-2021-25675

An attacker with local access to the system could cause a Denial-of-Service condition in the application when it is used to open a specially crafted file. As a consequence, a divide by zero operation could occur and cause the application to terminate unexpectedly and must be restarted to restore the service.

CVSS v3.1 Base Score	5.5
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:P/RL:W/RC:C
CWE	CWE-369: Divide By Zero

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 (2021-03-09): Publication Date

TERMS OF USE