SSA-641963: Remote Code Execution Vulnerability in Multiple SIMATIC Software Products

Publication Date: 2021-07-13
Last Update: 2021-07-13
Current Version: V1.0
CVSS v3.1 Base Score: 7.8

SUMMARY

Multiple SIMATIC Software products are affected by a vulnerability that could allow an attacker to manipulate project files and remotely execute code.

Siemens has released updates for several affected products and recommends to update to the latest versions. Siemens recommends specific countermeasures for products where updates are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC PCS 7 V8.2 and earlier: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC PCS 7 V9.0: All versions < V9.0 SP3	Update to V9.0 SP3 or later version To obtain SIMATIC PCS 7 V9.0 SP3 contact your local customer support.
SIMATIC PDM: All versions < V9.2	Update to V9.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109794361/
SIMATIC STEP 7 V5.X: All versions < V5.6 SP2 HF3	Update to V5.6 SP2 HF3 or later version https://support.industry.siemens.com/cs/de/en/view/109779992/
SINAMICS STARTER (containing STEP 7 OEM version): All versions < V5.4 HF2	Update to V5.4 HF2 or later version https://support.industry.siemens.com/cs/us/en/view/109782792/

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 PCS 7 is a distributed control system (DCS) integrating SIMATIC WinCC, SIMATIC Batch, SIMATIC Route Control, OpenPCS7 and other components.

SIMATIC PDM (Process Device Manager) is an universal, manufacturer-independent tool for configuration, parameter assignment, commissioning, diagnostics and maintenance of intelligent process devices (actors, sensors) and automation components (remote I/Os, multiplexer, process control units, compact controller).

SIMATIC STEP 7 V5.X is the classic engineering software to configure and program SIMATIC S7-300/S7-400/C7/WinAC controllers.

STARTER is the drive engineering tool for parameterizing and commissioning.

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-2021-31893

The affected software contains a buffer overflow vulnerability while handling certain files that could allow a local attacker to trigger a denial-of-service condition or potentially lead to remote code execution.

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Uri Katz from Claroty for coordinated disclosure

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 (2021-07-13): Publication Date

TERMS OF USE