

SSA-689942: Denial-of-Service and DLL Hijacking Vulnerabilities in Multiple SIMATIC Software Products

Publication Date: 2020-06-09
 Last Update: 2020-12-08
 Current Version: V1.2
 CVSS v3.1 Base Score: 7.8

SUMMARY

Multiple SIMATIC Software products are affected by two vulnerabilities that could allow an attacker to manipulate project files that may lead to Remote Code Execution or Denial-of-Service attacks.

Siemens has released updates to some of the affected products and recommends that customers update to the latest version. Siemens is preparing further updates and recommends specific workarounds and mitigations until patches are 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 or upgrade to a newer SIMATIC PCS 7 version |
| SIMATIC PCS 7 V9.0: All versions < V9.0 SP3 | Update to V9.0 SP3. To obtain SIMATIC PCS 7 V9.0 SP3 contact your local support. |
| SIMATIC PDM: All versions | See recommendations from section Workarounds and Mitigations |
| 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 STEP 7 V5.X is the classic engineering software to configure and program SIMATIC S7-300/S7-400/C7/WinAC controllers.

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).

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-2020-7585

A DLL Hijacking vulnerability could allow a local attacker to execute code with elevated privileges.

The security vulnerability could be exploited by an attacker with local access to the affected systems. Successful exploitation requires user privileges but no user interaction. The vulnerability could allow an attacker to compromise the availability of the system as well as to have access to confidential information.

| | |
|----------------------|--|
| 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-427: Uncontrolled Search Path Element |

Vulnerability CVE-2020-7586

A buffer overflow vulnerability could allow a local attacker to cause a Denial-of-Service situation.

The security vulnerability could be exploited by an attacker with local access to the affected systems. Successful exploitation requires user privileges but no user interaction. The vulnerability could allow an attacker to compromise the availability of the system as well as to have access to confidential information.

| | |
|----------------------|--|
| 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-122: Heap-based 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 (2020-06-09): Publication Date
V1.1 (2020-07-14): Added solution for SIMATIC PCS 7 V9.0
V1.2 (2020-12-08): Corrected affected version and patch link for SINAMICS STARTER

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.