SSA-188491: DLL Hijacking Vulnerabilities in Siemens Software Center

Publication Date: 2023-08-08
Last Update: 2023-08-08
Current Version: V1.0
CVSS v3.1 Base Score: 7.8

SUMMARY

Multiple DLL Hijacking vulnerabilities in Siemens Software Center (SSC) could allow a local attacker to execute code with elevated privileges.

Siemens has released an update for the Siemens Software Center and recommends to update to the latest version.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Siemens Software Center: All versions < V3.0	Update to V3.0 or later version (Existing installations of SSC will be prompted to update whenever a new version is available. The latest version can also be downloaded in the respective link) https://www.sw.siemens.com/en-US/siemens-software-center/ See further 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:

- Harden the application host to prevent local access by untrusted personnel

Product-specific remediations or mitigations can be found in the section Affected Products and Solution. Please follow the General Security Recommendations.

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

Siemens Software Center allows you to download, install, and activate purchased software. You can also update your software as new versions become available and launch free trials.

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-2021-41544

A DLL Hijacking vulnerability could allow a local attacker to execute code with elevated privileges by placing a malicious DLL in one of the directories on the DLL search path.

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-2022-25634

Qt through 5.15.8 and 6.x through 6.2.3 can load system library files from an unintended working directory.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

ACKNOWLEDGMENTS

Siemens thanks the following party for its efforts:

- Samuel Hanson from Dragos for reporting the vulnerabilities

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 (2023-08-08): Publication Date

TERMS OF USE