Siemens Security Advisory by Siemens ProductCERT

SSA-282044: DLL Hijacking Vulnerability in Siemens Web Installer used by the Online Software Delivery

Publication Date:	2025-08-12
Last Update:	2026-02-10
Current Version:	V1.6
CVSS v3.1 Base Score:	7.8
CVSS v4.0 Base Score:	8.5

▼ SUMMARY

The installers used to install several Siemens products are affected by a DLL hijacking vulnerability. This could allow an attacker to execute arbitrary code when a legitimate user installs an application that uses the affected installer component. This vulnerability poses a risk only during setup and installation phase of the affected applications downloaded e.g. via OSD (Online Software Delivery).

Siemens has released new versions for several affected products and recommends using the latest versions during setup and installation. Siemens is preparing further fix versions and recommends specific countermeasures for products where fixes are not, or not yet available.

▼ KNOWN AFFECTED PRODUCTS

Un-/Collapse All

Affected Product and Versions	Remediation
Automation License Manager	Show more details
CEMAT V10.0 All versions affected by CVE-2025-30033	Currently no fix is planned See further recommendations from section Mitigations
CP PtP Param configuring interface All versions affected by CVE-2025-30033	Currently no fix is available See further recommendations from section Mitigations
Create MyConfig (CMC) All versions < V6.9 affected by CVE-2025-30033	Update to V6.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109955311/ See further recommendations from section Mitigations
Energy Support Library (EnSL) All versions affected by CVE-2025-30033	Currently no fix is planned See further recommendations from section Mitigations
FM Configuration Package All versions affected by CVE-2025-30033	Currently no fix is available See further recommendations from section Mitigations
Modular PID CTRL Tool All versions affected by CVE-2025-30033	Currently no fix is available See further recommendations from section Mitigations

MultiFieldbus Configuration Tool (MFCT) All versions < V1.5.5.0 affected by CVE-2025-30033	Update to V1.5.5.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109773881/ See further recommendations from section Mitigations
OpenPCS 7	Show more details
Siemens Network Planner (SINETPLAN) All versions affected by CVE-2025-30033	Currently no fix is available See further recommendations from section Mitigations
SIMATIC Automation Tool All versions affected by CVE-2025-30033	Currently no fix is available See further recommendations from section Mitigations
SIMATIC Automation Tool SDK Windows All versions affected by CVE-2025-30033	Currently no fix is available See further recommendations from section Mitigations
SIMATIC BATCH	Show more details
SIMATIC eaSie Core Package (6DL5424-0AX00-0AV8) All versions affected by CVE-2025-30033	Currently no fix is available See further recommendations from section Mitigations
SIMATIC eaSie Document Skills All versions affected by CVE-2025-30033	Currently no fix is available See further recommendations from section Mitigations
SIMATIC eaSie PCS 7 Skill Package (6DL5424-0BX00-0AV8) All versions affected by CVE-2025-30033	Currently no fix is available See further recommendations from section Mitigations
SIMATIC eaSie Workflow Skills All versions affected by CVE-2025-30033	Currently no fix is available See further recommendations from section Mitigations
SIMATIC Logon	Show more details
SIMATIC Management Agent All versions < V9.1 SP1 Upd8 affected by CVE-2025-30033	Update to V9.1 SP1 Upd8 or later version https://support.industry.siemens.com/cs/ww/en/view/109812242/ See further recommendations from section Mitigations
SIMATIC Management Console All versions < V9.1 SP1 Upd8 affected by CVE-2025-30033	Update to V9.1 SP1 Upd8 or later version https://support.industry.siemens.com/cs/ww/en/view/109812242/ See further recommendations from section Mitigations
SIMATIC NET PC Software	Show more details
SIMATIC ODK 1500S All versions affected by CVE-2025-30033	Currently no fix is planned See further recommendations from section Mitigations
SIMATIC PCS 7	Show more details

SIMATIC PCS 7 Advanced Process Faceplates V9.1 All versions < V9.1 SP2 Upd4 affected by CVE-2025-30033	Update to V9.1 SP2 Upd4 or later version https://support.industry.siemens.com/cs/ww/en/view/109812242/ See further recommendations from section Mitigations
SIMATIC PCS 7 Advanced Process Functions	Show more details
SIMATIC PCS 7 Advanced Process Graphics	Show more details
SIMATIC PCS 7 Advanced Process Library incl. Faceplates V10.0 All versions affected by CVE-2025-30033	Currently no fix is available See further recommendations from section Mitigations
SIMATIC PCS 7 Advanced Process Library V9.1 All versions < V9.1 SP2 Upd6 affected by CVE-2025-30033	Update to V9.1 SP2 Upd6 or later version https://support.industry.siemens.com/cs/ww/en/view/109812242/ See further recommendations from section Mitigations
SIMATIC PCS 7 Basis Faceplates V9.1 All versions < V9.1 SP2 Upd2 affected by CVE-2025-30033	Update to V9.1 SP2 Upd2 or later version https://support.industry.siemens.com/cs/ww/en/view/109812242/ See further recommendations from section Mitigations
SIMATIC PCS 7 Basis Library	Show more details
SIMATIC PCS 7 Industry Library	Show more details
SIMATIC PCS 7 Logic Matrix	Show more details
SIMATIC PCS 7 MPC Configurator All versions affected by CVE-2025-30033	Currently no fix is available See further recommendations from section Mitigations
SIMATIC PCS 7 PowerControl All versions affected by CVE-2025-30033	Currently no fix is available See further recommendations from section Mitigations
SIMATIC PCS 7 Standard Chemical Library	Show more details
SIMATIC PCS 7 TeleControl All versions affected by CVE-2025-30033	Currently no fix is available See further recommendations from section Mitigations
SIMATIC PCS 7/OPEN OS V9.1 All versions affected by CVE-2025-30033	Currently no fix is available See further recommendations from section Mitigations
SIMATIC PCS neo	Show more details
SIMATIC PDM	Show more details
SIMATIC PDM Maintenance Station V5.0 All versions affected by CVE-2025-30033	Currently no fix is available See further recommendations from section Mitigations

SIMATIC Process Function Library (PFL) V4.0 All versions affected by CVE-2025-30033	Currently no fix is planned See further recommendations from section Mitigations
SIMATIC Process Historian	Show more details
SIMATIC ProSave	Show more details
SIMATIC Route Control	Show more details
SIMATIC S7 F Systems	Show more details
SIMATIC S7-1500 Software Controller	Show more details
SIMATIC S7-Fail-safe Configuration Tool (S7-FCT) All versions < V4.0.1 affected by CVE-2025-30033	Update to V4.0.1 or later version https://support.industry.siemens.com/cs/ww/en/view/109762827/ See further recommendations from section Mitigations
SIMATIC S7-PCT All versions < V3.5 SP4 Update 1 affected by CVE-2025-30033	Update to V3.5 SP4 Update 1 or later version https://support.industry.siemens.com/cs/ww/en/view/32469496/ See further recommendations from section Mitigations
SIMATIC S7-PLCSIM	Show more details
SIMATIC S7-PLCSIM Advanced All versions < V7.0 Update 1 affected by CVE-2025-30033	Update to V7.0 Update 1 or later version https://support.industry.siemens.com/cs/ww/en/view/109988436/ See further recommendations from section Mitigations
SIMATIC Safety Matrix All versions affected by CVE-2025-30033	Currently no fix is available See further recommendations from section Mitigations
SIMATIC STEP 7 CFC	Show more details
SIMATIC STEP 7 V5.7 All versions affected by CVE-2025-30033	Currently no fix is available See further recommendations from section Mitigations
SIMATIC Target All versions affected by CVE-2025-30033	Currently no fix is available See further recommendations from section Mitigations
SIMATIC WinCC	Show more details
SIMATIC WinCC flexible ES All versions affected by CVE-2025-30033	Currently no fix is planned See further recommendations from section Mitigations
SIMATIC WinCC Runtime Advanced All versions < V17 Update 9 affected by CVE-2025-30033	Update to V17 Update 9 or later version https://support.industry.siemens.com/cs/ww/en/view/109800912/ See further recommendations from section Mitigations

SIMATIC WinCC Runtime Professional All versions < V21 affected by CVE-2025-30033	Update to V21 or later version https://support.industry.siemens.com/cs/ww/en/view/109991139/ See further recommendations from section Mitigations
SIMATIC WinCC Runtime Professional V20 All versions affected by CVE-2025-30033	Currently no fix is available See further recommendations from section Mitigations
SIMATIC WinCC TeleControl All versions affected by CVE-2025-30033	Currently no fix is available See further recommendations from section Mitigations
SIMATIC WinCC Unified Line Coordination All versions < V20 affected by CVE-2025-30033	Update to V20 or later version https://support.industry.siemens.com/cs/ww/en/view/109987448/ See further recommendations from section Mitigations
SIMATIC WinCC Unified Sequence All versions < V20 affected by CVE-2025-30033	Update to V20 or later version https://support.industry.siemens.com/cs/ww/en/view/109987448/ See further recommendations from section Mitigations
SIMATIC D7-SYS All versions affected by CVE-2025-30033	Currently no fix is available See further recommendations from section Mitigations
SIMIT Rapid Tester All versions affected by CVE-2025-30033	Currently no fix is available See further recommendations from section Mitigations
SIMIT Simulation Platform All versions affected by CVE-2025-30033	Currently no fix is available See further recommendations from section Mitigations
SINEC NMS All versions < V4.0 affected by CVE-2025-30033	Update to V4.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109989514/ See further recommendations from section Mitigations
SINEMA Remote Connect Client All versions affected by CVE-2025-30033	Currently no fix is available See further recommendations from section Mitigations
SITRANS All versions affected by CVE-2025-30033	Currently no fix is available See further recommendations from section Mitigations
Standard PID CTRL Tool All versions affected by CVE-2025-30033	Currently no fix is available See further recommendations from section Mitigations
TeleControl Server Basic V3.1 All versions < V3.1.2.2 affected by CVE-2025-30033	Update to V3.1.2.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109987362/ See further recommendations from section Mitigations

TIA Administrator All versions < V3.0.6 affected by CVE-2025-30033	Update to V3.0.6 or later version https://support.industry.siemens.com/cs/ww/en/view/109825038/ See further recommendations from section Mitigations
TIA Portal Cloud Connector All versions < V2.3 affected by CVE-2025-30033	Update to V2.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109780755/ See further recommendations from section Mitigations
TIA Project-Server All versions < V2.2 affected by CVE-2025-30033	Update to V2.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109810588/ See further recommendations from section Mitigations
TIA Project-Server V17 All versions affected by CVE-2025-30033	Currently no fix is planned See further recommendations from section Mitigations
Totally Integrated Automation Portal (TIA Portal)	Show more details
WinCC Panel Image Setup All versions < V17 Update 9 affected by CVE-2025-30033	Update to V17 Update 9 or later version https://support.industry.siemens.com/cs/ww/en/view/109825750/ See further recommendations from section Mitigations

▼ MITIGATIONS

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

- Harden the application host to prevent local access by untrusted personnel
- Install applications only from an empty directory, thereby minimizing the likelihood of malicious DLLs being present

Product-specific remediations or mitigations can be found in the section Known Affected Products.
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

▼ VULNERABILITY DESCRIPTION

Un-/Collapse All

This chapter describes all vulnerabilities (CVE-IDs) addressed in this security advisory. Wherever applicable, it also documents the product-specific impact of the individual vulnerabilities.

▼ Vulnerability CVE-2025-30033

The affected setup component is vulnerable to DLL hijacking. This could allow an attacker to execute arbitrary code when a legitimate user installs an application that uses the affected setup component.

CVSS v3.1 Base Score	7.8
CVSS v3.1 Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
CVSS v4.0 Base Score	8.5
CVSS v4.0 Vector	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N
CWE	CWE-427: Uncontrolled Search Path Element

▼ ACKNOWLEDGMENTS

Siemens thanks the following party for its efforts:

- Sahil Shah from National Forensic Sciences University for reporting the vulnerability

▼ ADDITIONAL INFORMATION

Siemens uses an internal software component to bundle Siemens software into self-contained installer executables. This component, called "Siemens Web Installer Application (SIWA)", which is vulnerable to DLL hijacking. To ensure no untrusted DLL files are in the setup directory, install applications only from a directory containing only the installer file. This minimizes the likelihood of malicious DLLs being present.

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	(2025-08-12):	Publication Date
V1.1	(2025-09-09):	Added Sahil Shah to acknowledgment; Added fix for SIMATIC Energy Suite V19, SIMATIC Energy Suite V20, SIMATIC MTP CREATOR V4.x, SIMATIC Control Function Library (CFL) V3.x, TIA Portal Test Suite V19, TIA Portal Test Suite V20, SIMATIC WinCC Visualization Architect V19, SIMATIC WinCC Visualization Architect V20, SIMATIC S7-PCT; Updated No fix planned for SIMATIC ProSave V17,SIMATIC WinCC flexible ES, SIMATIC Control Function Library (CFL) V1.x, SIMATIC Control Function Library (CFL) V2.x
V1.2	(2025-10-14):	Added fix for MTP Creator V2.x, CFL V4.x, Simatic WinCC Unified Line Coordination and Simatic WinCC Unified Sequence
V1.3	(2025-11-11):	Added Fixes for PCS 7 Logic Matrix V9.1, PCS7 Advanced Process Faceplates V9.1, SIMATIC PCS 7 Basis Faceplates V9.1 PCS 7 Basis Library V9.1, SIMATIC Management Agent V9.1, SIMATIC Management Console V9.1, PCS 7 V9.1, PCS 7 V10.0
V1.4	(2025-12-09):	Added fixes for TIA Project-Server, TIA Portal Cloud Connector, SIMATIC MTP CREATOR V5.x, SIMATIC S7-1500 Software Controller V3, Simatic Prosave, TIA Portal V20, V19, and V17 and updated Energy suite V17 and V18, SIMATIC S7-1500 Software Controller V2 with no fix planned
V1.5	(2026-01-13):	Added fixes for WinCC Panel Image Setup, SIMATIC WinCC Runtime Advanced, SIMATIC WinCC Runtime Professional, SIMATIC WinCC Visualization Architect (SiVArc) V17, SIMATIC Process Historian 2024, SIMATIC PCS 7 Basis Library V10.0, SIMATIC Logon V2.0, SIMATIC PDM V9.3, and MultiFieldbus Configuration Tool (MFCT); Clarified that no fix is planned for TIA Project-Server V17

V1.6	(2026-02-10):	Updated remediation for SIMATIC ODK 1500S and SIMATIC S7-PLCSIM V17, V18, V19 to 'No fix planned' and added fix version for Create MyConfig (CMC)

▼ TERMS OF USE