Vulnerability Analysis: Siemens Web Installer. DLL Hijacking vulnerability you should not worry about

Version: 1.2 (16.03.2026)

Vulnerability data analysis for inaccuracies to help avoid incorrect vulnerability assessment and ineffective mitigation.

Executive Summary

CVE-2025-30033	UNCONTROLLED SEARCH PATH ELEMENT (CWE-427)
Severity Kaspersky ICS CERT	**0.0 (None)**
Severity Vendor	**7.8 (High)**

Siemens have published a cybersecurity advisory on the set of products using Siemens Web Installer, addressing a DLL search order hijacking vulnerability. The vendor assesses its severity as High.

We have analyzed the vulnerability and, based on our findings, have reassessed its score as 0.0 (None). To exploit the vulnerability, an attacker would need to have already gained highly privileged access to the workstation. With these privileges, the attacker could gain full control over the system and execute malicious code as SYSTEM, without needing to exploit any other vulnerability.

Given this, we recommend focusing on measures that prevent unauthorized access to workstations, rather than prioritizing remediation of this specific CVE.

Affected products	See affected products table
Remediation	Implement protection measures preventing unauthorized access to workstations.

For more information, please contact: ics-cert@kaspersky.com

In This Advisory

Technical Details

Product Description

Automation License Manager (ALM) centrally manages license keys for various Siemens software products.

SIMATIC NET PC software is a software product that is sold separately and implements the communications product from SIMATIC NET.

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

SIMATIC PCS 7 TeleControl is a server based software for the integration of outstations for monitoring and controlling highly remote plant units (referred to as RTUs, usually with a small or medium degree of automation) into the PCS 7 control system. This is carried out by means of telecontrol protocols over a WAN (Wide Area Network).

SIMATIC PCS neo is a distributed control system (DCS).

SIMATIC S7-1500 Software Controller is a SIMATIC software controller for PC-based automation solutions.

SIMATIC S7-PLCSIM Advanced simulates S7-1200, S7-1500 and a few other PLC derivatives. Includes full network access to simulate the PLCs, even in virtualized environments.

SIMATIC S7-PLCSIM simulates S7-1200, S7-1500 and a few other PLC derivatives and is shipped as part of SIMATIC STEP 7.

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

SIMATIC TeleControl for WinCC is a server based software for the integration of outstations for monitoring and controlling highly remote plant units (referred to as RTUs, usually with a small or medium degree of automation) into the WinCC SCADA system. This is carried out by means of telecontrol protocols over a WAN (Wide Area Network).

SIMATIC WinCC is a supervisory control and data acquisition (SCADA) system.

SIMATIC WinCC Runtime Advanced is a visualization runtime platform used for operator control and monitoring of machines and plants.

SIMATIC WinCC Runtime Professional is a visualization runtime platform used for operator control and monitoring of machines and plants.

SINEC NMS is a new generation of the Network Management System (NMS) for the Digital Enterprise. This system can be used to centrally monitor, manage, and configure networks.

SINEMA Remote Connect is a management platform for remote networks that enables the simple management of tunnel connections (VPN) between headquarters, service technicians, and installed machines or plants. It provides both the Remote Connect Server, which is the server application, and the Remote Connect Client, which is an OpenVPN client for optimal connection to SINEMA Remote Connect Server.

TeleControl Server Basic allows remote monitoring and control of plants via WAN/LAN.

TIA Administrator is a web-based framework that can incorporate different function modules for administrative tasks, as well as functions for managing SIMATIC software and licenses.

TIA Project-Server formerly known as TIA Multiuser Server allows to work with multiple users together and simultaneously on a project.

Totally Integrated Automation Portal (TIA Portal) is a PC software that provides access to the complete range of Siemens digitalized automation services, from digital planning and integrated engineering to transparent operation.

Analysis

On August 12, 2025, Siemens published a security advisory describing vulnerability regarding a range of software products revolved around DLL search order hijacking. Vendor rated this vulnerability as 7.8 High with AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H CVSS vector.

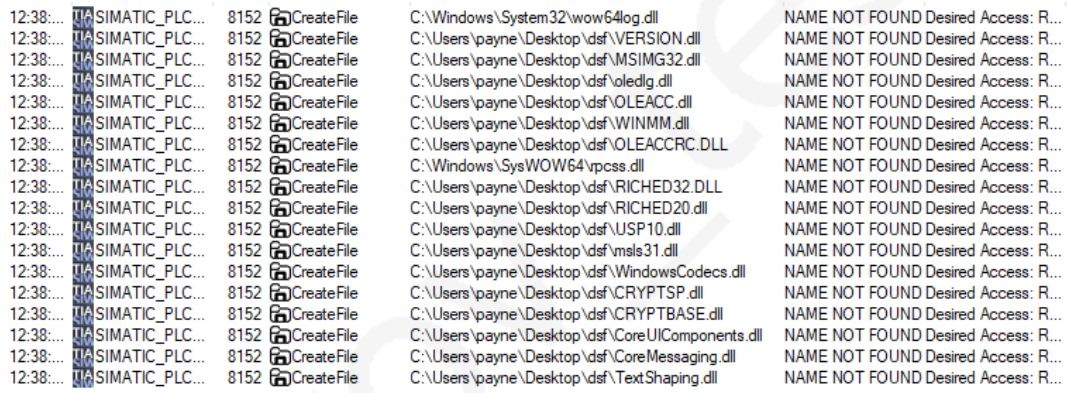
According to the description in the security advisory, vulnerability allows for DLLs to be executed when a legitimate user installs an application downloaded via Online Software Delivery.

> *DLL search order hijacking is possible due to the Windows operating system's search order of DLLs. For example, application.exe residing in the C:\Program Files\Application folder may need to load the helper.dll, which may be located on the file system. Loading DLLs can be done in several ways, such as using absolute or relative paths to the required DLL. An absolute path provides a full, exact path to DLL without any ambiguity. A relative path, on the other hand, will utilize the Windows operating system's DLL search order, which will start searching for the required DLL in the same folder where application.exe is located. Then, if the DLL is not found, search will continue in C:\Windows\System, C:\Windows\System32 and so on (for more on Windows DLL search order look here). The problem arises when the attacker manages to place a malicious DLL with a proper name (helper.dll in our example) in the folder that will be checked by the operating system before the folder where the legitimate DLL is stored, causing a malicious DLL to be loaded into the memory. For DLL hijacking vulnerability to be exploited, the application has to make a call for a DLL from a location on the system that is accessible to the attacker – specifically, a location where an attacker can write files to.*

Applications downloaded via Online Software Delivery are unique in that they include Siemens Web Installer (SIWA) binary for self-insallation possibilities in addition to the downloaded program itself. And as stated by vendor in advisory, it is SIWA that contains the vulnerable logic related to DLL files.

We have analyzed multiple affected products downloaded via OSD for SIWA presence and decided to focus on SIMATIC S7-PLCSIM Advanced V3, which contains an unpatched SIWA version, as a research object for the analysis.

The vulnerable SIMATIC S7-PLCSIM installer makes numerous calls to various DLLs, namely, it attempts to load version.dll, msimg32.dll, oledlg.dll, oleacc.dll, winmm.dll, oleaccrc.dll, riched32.dll, riched20.dll, usp10.dll, msls31.dll, WindowsCodecs.dll, crypstp.dll, cryptbase.dll, CoreMessaging.dll, CoreUIComponents.dll and TextShaping.dll (as highlighted in Fig. 1).

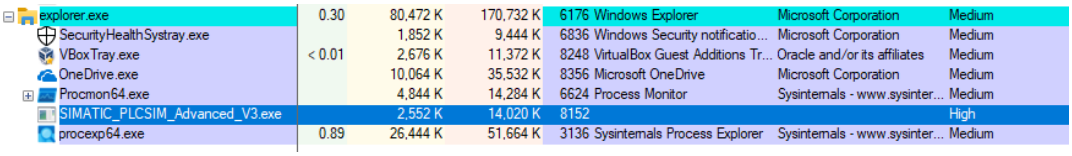


12:38:...	SIMATIC_PLC...	8152	CreateFile	C:\Windows\System32\wow64log.dll	NAME NOT FOUND Desired Access: R...
12:38:...	SIMATIC_PLC...	8152	CreateFile	C:\Users\payne\Desktop\dsf\VERSION.dll	NAME NOT FOUND Desired Access: R...
12:38:...	SIMATIC_PLC...	8152	CreateFile	C:\Users\payne\Desktop\dsf\MSIMG32.dll	NAME NOT FOUND Desired Access: R...
12:38:...	SIMATIC_PLC...	8152	CreateFile	C:\Users\payne\Desktop\dsf\oledlg.dll	NAME NOT FOUND Desired Access: R...
12:38:...	SIMATIC_PLC...	8152	CreateFile	C:\Users\payne\Desktop\dsf\OLEACC.dll	NAME NOT FOUND Desired Access: R...
12:38:...	SIMATIC_PLC...	8152	CreateFile	C:\Users\payne\Desktop\dsf\WINMM.dll	NAME NOT FOUND Desired Access: R...
12:38:...	SIMATIC_PLC...	8152	CreateFile	C:\Users\payne\Desktop\dsf\OLEACCRC.DLL	NAME NOT FOUND Desired Access: R...
12:38:...	SIMATIC_PLC...	8152	CreateFile	C:\Windows\SysWOW64\vpcss.dll	NAME NOT FOUND Desired Access: R...
12:38:...	SIMATIC_PLC...	8152	CreateFile	C:\Users\payne\Desktop\dsf\RICHED32.DLL	NAME NOT FOUND Desired Access: R...
12:38:...	SIMATIC_PLC...	8152	CreateFile	C:\Users\payne\Desktop\dsf\RICHED20.dll	NAME NOT FOUND Desired Access: R...
12:38:...	SIMATIC_PLC...	8152	CreateFile	C:\Users\payne\Desktop\dsf\USP10.dll	NAME NOT FOUND Desired Access: R...
12:38:...	SIMATIC_PLC...	8152	CreateFile	C:\Users\payne\Desktop\dsf\msls31.dll	NAME NOT FOUND Desired Access: R...
12:38:...	SIMATIC_PLC...	8152	CreateFile	C:\Users\payne\Desktop\dsf\WindowsCodecs.dll	NAME NOT FOUND Desired Access: R...
12:38:...	SIMATIC_PLC...	8152	CreateFile	C:\Users\payne\Desktop\dsf\CRYPTSP.dll	NAME NOT FOUND Desired Access: R...
12:38:...	SIMATIC_PLC...	8152	CreateFile	C:\Users\payne\Desktop\dsf\CRYPTBASE.dll	NAME NOT FOUND Desired Access: R...
12:38:...	SIMATIC_PLC...	8152	CreateFile	C:\Users\payne\Desktop\dsf\CoreUIComponents.dll	NAME NOT FOUND Desired Access: R...
12:38:...	SIMATIC_PLC...	8152	CreateFile	C:\Users\payne\Desktop\dsf\CoreMessaging.dll	NAME NOT FOUND Desired Access: R...
12:38:...	SIMATIC_PLC...	8152	CreateFile	C:\Users\payne\Desktop\dsf\TextShaping.dll	NAME NOT FOUND Desired Access: R...

Figure 1 – SIMATIC_PLCSIM_Advanced_V3.exe DLL call history

At first, the binary attempts to load these DLL files from the current folder from which it was launched (C:\Users\payne\Desktop\dsf, for example), which is protected from write access by other users. If these files are not found in the current folder, the binary will then look for them in the system folders such as C:\Windows\SysWOW64\ and C:\Windows\System\. Because all DLL files searched by the binary are found in the Windows folder, Windows search order never checks the PATH variable. Therefore, exploitation can only occur if malicious DLL files are injected into the current folder where the installer was executed.

According to information from Process Explorer (Fig. 2), the SIMATIC_PLCSIM_Advanced_V3.exe binary launched by a user runs with High integrity level – the default behavior for applications running with elevated rights. This means a low-privileged attacker can execute code with elevated privileges if he manages to place a malicious DLL library in the folder from which the Siemens Web Installer is executed.



explorer.exe	0.30	80,472 K	170,732 K	6176 Windows Explorer	Microsoft Corporation	Medium
SecurityHealthSystray.exe		1,852 K	9,444 K	6836 Windows Security notificatio...	Microsoft Corporation	Medium
VBoxTray.exe	< 0.01	2,676 K	11,372 K	8248 VirtualBox Guest Additions Tr...	Oracle and/or its affiliates	Medium
OneDrive.exe		10,064 K	35,532 K	8356 Microsoft OneDrive	Microsoft Corporation	Medium
Procmon64.exe		4,844 K	14,284 K	6624 Process Monitor	Sysinternals - www.sysinter...	Medium
SIMATIC_PLCSIM_Advanced_V3.exe		2,552 K	14,020 K	8152		High
procexp64.exe	0.89	26,444 K	51,664 K	3136 Sysinternals Process Explorer	Sysinternals - www.sysinter...	Medium

Figure 2 – SIMATIC_PLCSIM_Advanced_V3.exe integrity level

However, the realism of the scenario with placing the DLL file in a folder from which an installer is launched remains in doubt, since by default these files are typically downloaded to the user's “Downloads” folder, which other users do not have write access to (unless they have elevated privileges). Based on our findings, there are no DLL calls that could be easily

exploited by a low-privileged attacker to achieve code execution with elevated privileges. All of the above leads us to conclude that there is no increase in access, no privileges gained, and no other negative impact — ultimately assigning the impact score of CVE-2025-30033 as 0.0 (None).

Conclusions

The severity of DLL hijacking vulnerability in Siemens products has been reduced to 0.0 (None). An attacker with elevated privileges can already cause significant damage to the system without exploiting this vulnerability. Therefore, the primary focus should be on preventing unauthorized access to workstations.

Affected Products and Updates

	Products	Mitigation
1.	**Automation License Manager** Versions after V6 and before V6.2 Update 3	✓ Vendor has released Automation License Manager V6.2 Update 3, which is not affected. *KL ICS CERT comment: Updating solely to address this vulnerability may not be necessary, given its negligible impact.*
2.	**OpenPCS 7** Versions V9.1.*, V10.0.*	Currently no fixed versions are available
3.	**SIMATIC NET PC Software** Versions before V20.0 Update 1	✓ Vendor has released SIMATIC NET PC Software V20.0 Update 1, which is not affected. *KL ICS CERT comment: Updating solely to address this vulnerability may not be necessary, given its negligible impact.*
4.	**SIMATIC PCS 7** Versions after 9.0.0.0 and before 9.1.1.8	✓ Update to V9.1 SP1 UC08 or later version https://support.industry.siemens.com/cs/ww/en/view/109812242 *KL ICS CERT comment: Updating solely to address this vulnerability may not be necessary, given its negligible impact.*
5.	**SIMATIC PCS 7** Versions after 10.0.0.0 and before 10.0.1.1	✓ Update to V10.0 SP1 UC01 or later version https://support.industry.siemens.com/cs/ww/en/view/109983445 *KL ICS CERT comment: Updating solely to address this vulnerability may not be necessary, given its negligible impact.*
6.	**SIMATIC PCS neo** Versions before V6.0 SP1	✓ Vendor has released SIMATIC PCS neo V6.0 SP1, which is not affected. *KL ICS CERT comment: Updating solely to address this vulnerability may not be necessary, given its negligible impact.*

	Products	Mitigation
7.	**SIMATIC Process Historian** Versions 2020, 2022, 2024	Currently no fixed versions are available
8.	**SIMATIC S7-1500 Software Controller v2** All versions	Currently no fixed versions are available
9.	**SIMATIC S7-1500 Software Controller v3** Versions before V31.1.5	✓ Update to V31.1.5 or later version https://support.industry.siemens.com/cs/ww/en/view/109478528/ *KL ICS CERT comment: Updating solely to address this vulnerability may not be necessary, given its negligible impact.*
10.	**SIMATIC S7-PLCSIM** Versions before V20 Update 1	✓ Vendor has released SIMATIC S7-PLCSIM V20.0 Update 1, which is not affected. *KL ICS CERT comment: Updating solely to address this vulnerability may not be necessary, given its negligible impact.*
11.	**SIMATIC S7-PLCSIM Advanced** Versions before V7.0 Update 1	✓ Vendor has released SIMATIC S7-PLCSIM Advanced V7.0 Update 1, which is not affected. *KL ICS CERT comment: Updating solely to address this vulnerability may not be necessary, given its negligible impact.*
12.	**SIMATIC STEP 7** Version V5.7	Currently no fixed versions are available
13.	**SIMATIC WinCC** Versions after V7.5 and before V8.1 Update 3	✓ Vendor has released SIMATIC WinCC V8.1 Update 3, which is not affected. *KL ICS CERT comment: Updating solely to address this vulnerability may not be necessary, given its negligible impact.*
14.	**SIMATIC WinCC Runtime Advanced** Versions before V17 Update 9	✓ Update to V17 Update 9 or later version https://support.industry.siemens.com/cs/ww/en/view/109800912/ *KL ICS CERT comment: Updating solely to address this vulnerability may not be necessary, given its negligible impact.*
15.	**SIMATIC WinCC Runtime Professional** Versions before V21	✓ Update to V21 or later version https://support.industry.siemens.com/cs/ww/en/view/109991139/ *KL ICS CERT comment: Updating solely to address this vulnerability may not be necessary, given its negligible impact.*
16.	**SINEC NMS** Versions before V4.0	✓ Vendor has released SINEC NMS V4.0, which is not affected. *KL ICS CERT comment: Updating solely to address this vulnerability may not be necessary, given its negligible impact.*

	Products	Mitigation
17.	**SINEMA Remote Connect Client** All versions	Currently no fixed versions are available
18.	**TeleControl Server Basic V3.1** Versions before V3.1.2.2	✓ Vendor has released TeleControl Server Basic V3.1.2.2, which is not affected. *KL ICS CERT comment: Updating solely to address this vulnerability may not be necessary, given its negligible impact.*
19.	**TIA Administrator** Versions before V3.0.6	✓ Vendor has released TIA Administrator V3.0.6, which is not affected. *KL ICS CERT comment: Updating solely to address this vulnerability may not be necessary, given its negligible impact.*
20.	**TIA Project-Server V17** All versions	Currently no fixed versions are available
21.	**TIA Project-Server** Versions before V2.2	✓ Update to V2.2 or later version https://support.industry.siemens.com/cs/ww/en/view/109810588/ *KL ICS CERT comment: Updating solely to address this vulnerability may not be necessary, given its negligible impact.*
22.	**Totally Integrated Automation Portal (TIA Portal)** Versions V17, V18, V19, V20	Currently no fixed versions are available

Mitigations

Kaspersky ICS CERT recommendations	
Generic	Implement protection measures preventing unauthorized access to workstations.

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

References

Source	
Siemens	SSA-282044: DLL Hijacking Vulnerability in Siemens Web Installer used by the Online Software Delivery
NVD	CVE-2025-30033

Revision History

Date	Revision
12.09.2025	v1.0 Initial Release
13.02.2026	v1.1 Vulnerable product's versions were updated
16.03.2026	v1.2 Vulnerable product's versions were updated

Kaspersky Industrial Control Systems Cyber Emergency Response Team (Kaspersky ICS CERT) is a global project of Kaspersky aimed at coordinating the efforts of automation system vendors, industrial facility owners and operators, and IT security researchers to protect industrial enterprises from cyberattacks. Kaspersky ICS CERT devotes its efforts primarily to identifying potential and existing threats that target industrial automation systems and the industrial internet of things.

Kaspersky ICS CERT ics-cert@kaspersky.com