Siemens Software Center: Actively Exploited Flaw Puts OT Engineering Hosts at Risk

CVE-2026-110936 and CISA OT Advisories of 20 and 22 October 2026

26 October 2026 | Reference NST-2026-1026-001

1. What You Need to Know

On 19 October 2026, Siemens confirmed that CVE-2026-110936, a DLL side-loading vulnerability in Siemens Software Center, is being exploited in the wild. Software Center downloads, installs, licenses and updates Siemens engineering software, so it is commonly present on the engineering workstations that configure PLCs, HMIs and SCADA systems, one step from the control environment.

Attackers do not target existing installations. They deliver their own signed, older copy of Software Center with malicious DLLs, which the executable loads at start-up. Upgrading to 4.0.9.8 is required but does not stop this method, so it must be combined with a behaviour-based compromise review and execution controls on engineering workstations.

Why patching alone does not close this. Like bring-your-own-vulnerable-driver attacks, the adversary carries the vulnerable, trusted component with them. The 4.0.9.8 fix protects installed copies; what stops the campaign is blocking execution from user-writable paths and version-aware allow-listing of the Siemens binary.

Overall rating	**HIGH (CVSS v4.0 8.4, CVSS v3.1 6.7, both scored for a local attacker with high privileges; actively exploited by having users run an attacker-supplied copy, so real-world risk exceeds the base scores)**
Affected component	Siemens Software Center, all versions before 4.0.9.8
Weakness	CWE-427, uncontrolled search path element, exploited as DLL side-loading
Potential impact	Arbitrary code execution with the privileges of the user running Software Center, typically an engineer with access to OT project files and controllers
Remediated release	Siemens Software Center 4.0.9.8 and later (Siemens ProductCERT advisory SSA-580366)
Exploitation status	**Exploited in the wild through the Romulus multi-platform ClickFix campaign; added to the CISA Known Exploited Vulnerabilities catalogue on 20 October 2026, with a federal remediation due date of 3 November 2026**

2. What Happened

Siemens disclosed the vulnerability on 15 October 2026 following a report by a Huntress Labs researcher and confirmed exploitation four days later. The chronology summarises the week's OT-relevant events as reported at the date of this advisory.

Date	Event
15 October 2026	Siemens publishes SSA-580366 for CVE-2026-110936 in Software Center, rated CVSS v4.0 8.4; version 4.0.9.8 is added as the fixed release in v1.1 on 17 October.
19 October 2026	Siemens updates SSA-580366 to version 1.2, confirms in-the-wild exploitation in the Romulus multi-platform ClickFix campaign, and links to a ProductCERT blog post that publishes network, file-hash and host indicators of compromise.
20 October 2026	CISA releases six ICS advisories, including WAGO OS Linux, Moxa AIG-302 ThingsPro Edge, Hitachi Energy MicroSCADA X SYS600, Hitachi Energy RTU500 and HMS/PEAK-System PCAN Windows drivers.
22 October 2026	CISA releases a larger Siemens-focused batch covering Industrial Edge, Industrial Edge App Publisher, SIMATIC S7-1500 PLC web servers and MFP CPUs, the .NET client library for the S7 Webserver API, WinCC, Capital Embedded AR Classic and building automation products.

Date	Event
22–23 October 2026	Arista discloses CVE-2026-114625 (SA-0199), an actively exploited CVSS v3.1 9.9 SQL injection in on-premises VeloCloud Orchestrator, the central management platform for VeloCloud SD-WAN deployments. CISA adds it to the KEV catalogue on 23 October.

ClickFix lures have users run a command themselves, bypassing attachment and macro controls. Pairing this with a signed industrial binary defeats reputation-based detection on the hosts that matter most in OT.

VeloCloud Orchestrator is not an OT product, but where SD-WAN connects plants and remote sites it controls the routing and access paths into them. It has had two earlier critical flaws in 2026, CVE-2026-16812 and CVE-2026-93952, both rated CVSS v3.1 10.0, confirmed by Arista as exploited and added to the CISA KEV catalogue.

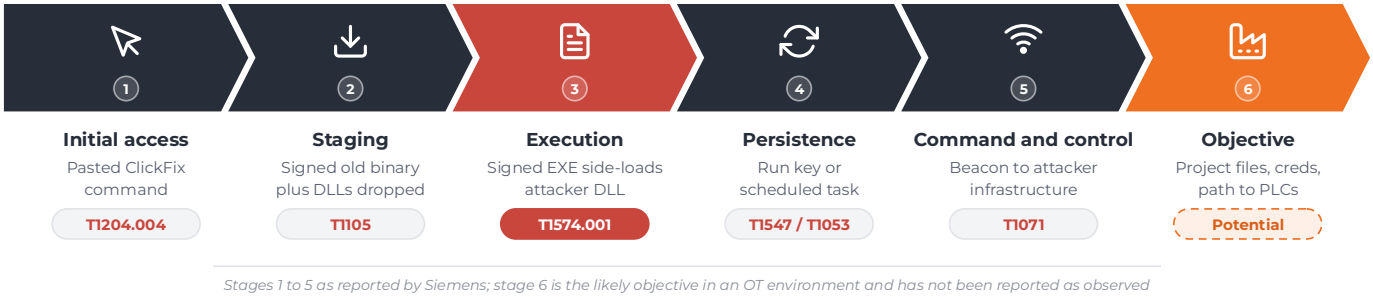
3. How the Vulnerability Works

When a Windows application loads a library without specifying its full path, the operating system resolves it through a defined search order, in which, after DLL redirection, API sets, manifest redirection, already-loaded modules and the Known DLLs list, the first directory searched is the one from which the application was loaded. Software Center versions before 4.0.9.8 load a number of libraries in this way. Any DLL with a matching name placed in the same directory as the executable is therefore loaded in preference to the legitimate copy, unless the library is a Known DLL or already loaded, and its code runs inside the Software Center process with the privileges of the user.

Because the vulnerable executable runs from any location, the attacker needs no access to an existing installation, only to place the signed binary and the malicious DLLs together in a user-writable folder and start it. The Siemens binary remains genuine and unmodified, so file hash, code signing and reputation checks continue to report it as trusted.

3.1 Observed Attack Chain

The decisive step is stage 3, where a binary every reputation service trusts loads code none of them has seen. Host evidence for each stage is in Section 5.2. Stage 3 is tagged T1574.001 (Hijack Execution Flow: DLL), which has covered DLL side-loading since MITRE merged the former T1574.002 into it in ATT&CK v17.



Stages 1 to 5 as reported by Siemens; stage 6 is the likely objective in an OT environment and has not been reported as observed

3.2 Consequence for Industrial Environments

Engineering workstations hold PLC and HMI project files and the credentials used to download logic, and are permitted to cross zone boundaries into Level 1 and 2. Code running as the engineer can alter project files, capture credentials and use the workstation's trust relationships to reach controllers. Engineering laptops that move between corporate and plant networks can carry a corporate-side compromise into the plant.

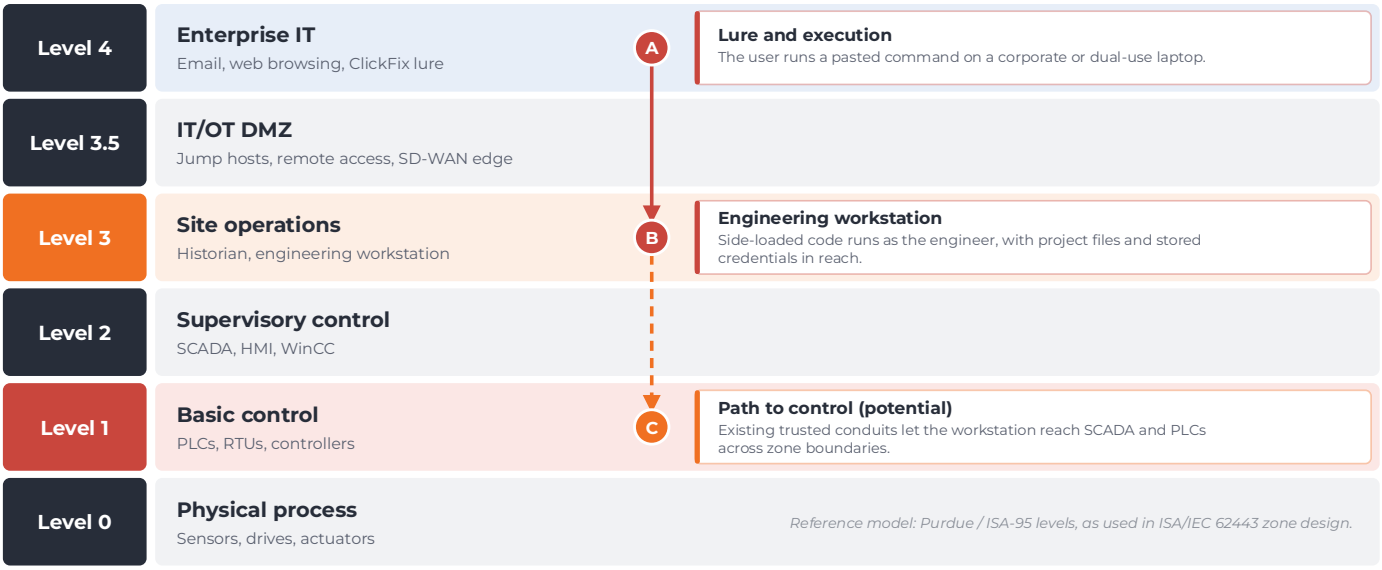


Figure: how a ClickFix compromise of an engineering workstation maps to the Purdue reference model

3.3 Indicators of Compromise

Siemens has published the following indicators. Search historical logs for the network indicators as well as blocking them.

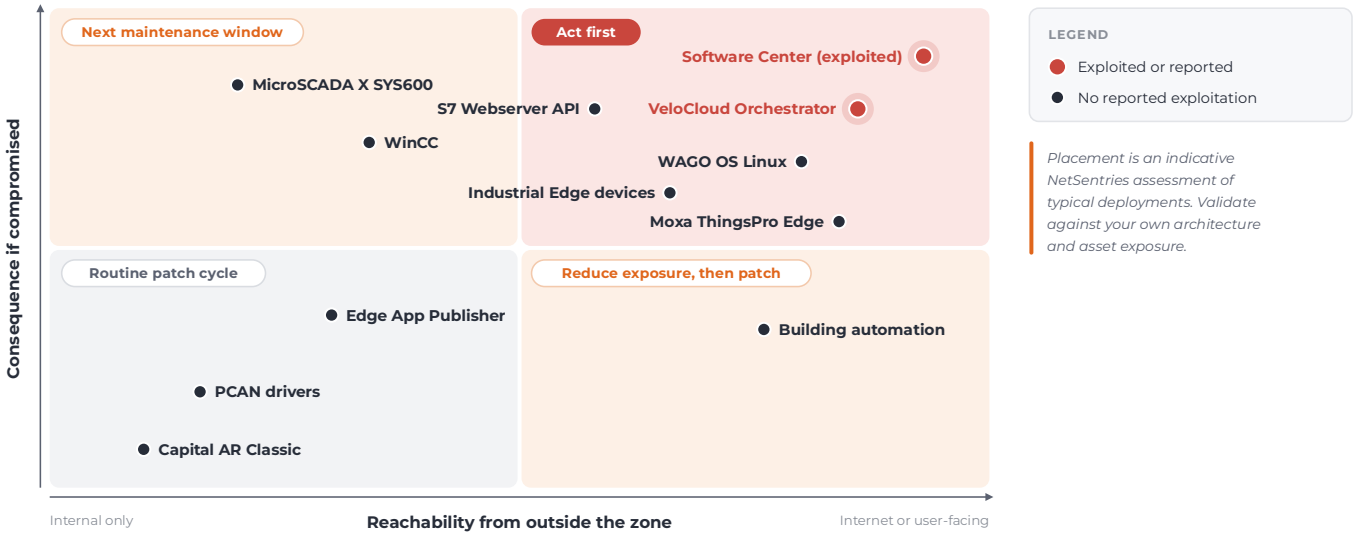
Type	Indicator	Where to Look
Network	**96.62.218[.]59**	Firewall, proxy and DNS logs; used for payload hosting and command and control
Network	**wizardexpensive[.]com**	DNS and proxy logs; used for payload hosting and command and control
Network	**2.27.248[.]127**	Firewall, proxy and DNS logs; inactive channel that distributed AllMyBasic.msi, so search history rather than relying on a block
Host	**SiemensSoftwareCenter.exe running from AppData\Local\Programs, started by msiexec.exe**	EDR process telemetry, with parent process and command line
Host	**activate.bak, statinfosta.DB, ftc.uml, FTSuite and SM Software Provisioning Service artefacts**	File system: beside the executable and under AppData\Local
File hash	**AllMyBasic.msi — SHA-256 f4d7c5321bb0d1bda439304a753bcf9b467b98ca53c7e9493b9c2c3451092e4a**	EDR file and installer telemetry, Downloads and Temp folders; malicious MSI package
File hash	**archive.dll — SHA-256 3fdcc7d7d049a89711fb31fb236940a1c5a09d899143ffd20c3c41fb1f2cf491**	EDR file and image-load telemetry, beside SiemensSoftwareCenter.exe; malicious side-loaded DLL

4. Who Is Affected

Organisations using Siemens engineering software such as TIA Portal, STEP 7 and WinCC should assume Software Center is on their engineering workstations and integrator laptops. As the attacker supplies the vulnerable copy, any Windows host that permits execution from user profile folders is also exposed.

4.1 Prioritising the Disclosures

CVSS scores describe a vulnerability in isolation. In OT environments, the order of remediation is better set by two factors: how easily an attacker can reach the asset from outside its zone, and what a compromise would allow them to do to the process. The matrix applies these factors to the products in this advisory. Assets in the upper right warrant attention first, while those in the lower right are often best addressed by removing their exposure before an update can be scheduled.



4.2 Disclosures in Scope

Industrial Edge App Publisher (CVE-2026-78556, CVE-2026-78557, fixed in 1.27.9) and PCAN drivers (six CVEs, fixed in 5.1.4) follow the routine patch cycle. Several products have no fix, or no planned fix, for some versions and must be managed by mitigation: Capital Embedded AR Classic 431-422 (CVE-2026-89208; R20-11 is fixed in V2303), APOGEE MBC/MEC and some Desigo PXC/PXM lines (CVE-2026-102073 to CVE-2026-102076, CVE-2026-89208), WinCC V7.5, several Industrial Edge Device Kit versions including V1.25, and MicroSCADA X SYS600 10.8 for CVE-2026-9853 and CVE-2026-9854. The matrix places Capital Embedded AR Classic by exposure and consequence, but its unfixed

versions still need mitigation rather than a routine update. The table lists the highest-priority products only: building automation, PCAN drivers, Industrial Edge App Publisher and Capital Embedded AR Classic appear in the matrix alone. The SIMATIC S7-1500 PLC web server and MFP CPUs (CISA CVSS v3 9.6 and 10, no fix available) and Hitachi Energy RTU500 are not plotted in the matrix and should be prioritised for mitigation wherever they are reachable from outside their zone.

Product	CVE	Exploitation	OT Relevance
Siemens Software Center	CVE-2026-110936	**Exploited**	Engineering workstations supporting industrial environments
Arista VeloCloud Orchestrator	CVE-2026-114625	**Exploited**	SD-WAN control plane where it connects plants and remote sites
Moxa AIG-302 ThingsPro Edge	CVE-2026-109812, CVE-2026-109813	**Not reported**	IIoT gateways bridging OT data to IT or cloud
WAGO OS Linux	CVE-2026-80466, CVE-2026-88850	**Not reported**	Controllers and edge devices with web management interfaces
Siemens Industrial Edge Device Kit and devices	CVE-2026-44414, CVE-2026-44415	**Not reported**	Edge compute connected to both plant and IT networks
Siemens .NET Client Library for SIMATIC S7 Webserver API	CVE-2026-85114, CVE-2026-85115	**Not reported**	Engineering and integration tools built on the library that connect to S7 PLCs
Siemens SIMATIC S7-1500 PLC web server	CVE-2026-63350 to CVE-2026-63357	**Not reported**	PLC web servers, where enabled and reachable; no fix available, so disable or restrict the web server
Siemens SIMATIC S7-1500 CPU 1518(F)-4 PN/DP MFP	Several hundred third-party CVEs (ICSA-26-295-11)	**Not reported**	Controllers with an additional GNU/Linux subsystem; no fix available, so limit shell access
Hitachi Energy MicroSCADA X SYS600	CVE-2026-9852, CVE-2026-9853, CVE-2026-9854	**Not reported**	Substation and grid SCADA
Hitachi Energy RTU500	CVE-2026-17539 et al. (ICSA-26-293-05)	**Not reported**	Substation and grid RTUs using IEC 60870-5-104; some fixed firmware is not yet available
Siemens WinCC	CVE-2026-59241	**Not reported**	HMI and SCADA at supervisory level

5. What You Should Do

5.1 Recommendations

CVE-2026-110936 and CVE-2026-114625 should be addressed first, as the two vulnerabilities here with confirmed exploitation, both listed in the CISA KEV catalogue. The compromise review and hardening steps follow in Sections 5.2 to 5.4.

Ref	Area	Recommendation
1	**Upgrade**	Identify every host with Siemens Software Center installed, including integrator and contractor laptops, and confirm that version 4.0.9.8 or later is in place. Existing installations update when the application starts, but this should be verified through software inventory rather than assumed.
2	**Block**	Block 96.62.218[.]59, wizardexpensive[.]com and 2.27.248[.]127 at the perimeter, proxy and DNS layers, search historical logs for connections to all three, and sweep endpoints for the published SHA-256 hashes: AllMyBasic.msi f4d7c5321bb0d1bda439304a753bcf9b467b98ca53c7e9493b9c2c3451092e4a and archive.dll 3fdcc7d7d049a89711fb31fb236940a1c5a09d899143ffd20c3c41fb1f2cf491.
3	**SD-WAN**	Upgrade on-premises VeloCloud Orchestrator to 5.2.3.18, 6.1.3.10 or 6.4.2.12 or later to fix the actively exploited CVE-2026-114625 (CISA KEV remediation was due 26 October 2026 and is now overdue), as releases that fixed CVE-2026-16812 or CVE-2026-93952 remain vulnerable; on the 6.1 train, confirm with Arista that CVE-2026-93952 is also fixed; restrict its management interface to a management network or an MFA-protected jump host, and review its audit logs for unexpected administrators, edge enrolments and policy changes.
4	**Exposure**	Confirm that WAGO web interfaces, Moxa ThingsPro Edge, Siemens Industrial Edge, SIMATIC S7 web servers, VeloCloud Orchestrator and remote engineering services are not reachable from the internet, and assign an owner to each finding.
5	**Patch**	Validate updates for the remaining products in Section 4 with the vendor or integrator and apply them in planned maintenance windows, starting with devices reachable from outside their zone. Where an update cannot yet be applied, disable unused web services and restrict management access to named engineering hosts.

5.2 Compromise Review

Base the review on behaviour and location, not on the hash of the legitimate Siemens executable. The telemetry below applies to hosts with Sysmon or an equivalent EDR. Sysmon network connection and image load logging are off by default and must be enabled in the Sysmon configuration.

Telemetry	What to Look For
Process creation (Sysmon 1)	SiemensSoftwareCenter.exe started from a user profile path, or with powershell.exe, cmd.exe, mshta.exe or msiexec.exe as its parent process.
Image load (Sysmon 7)	DLLs loaded by the Software Center process from its own directory that are unsigned, or signed by a party other than Siemens or Microsoft.
File creation (Sysmon 11)	Creation of activate.bak, statinfosta.DB or ftc.uml, or of executables and DLLs under AppData\Local\Programs.
Network and DNS (Sysmon 3, 22)	Connections or lookups to the published indicators, or outbound connections from Software Center to destinations other than Siemens infrastructure.
Persistence and user activity	Run keys or scheduled tasks (Sysmon 13, Event 4698) referencing a user-profile copy, and RunMRU entries containing pasted PowerShell or mshta commands.

Where activity is confirmed, isolate the host from corporate and OT networks, preserve evidence, remove persistence and reimage. Reset domain, engineering and controller credentials used on it, and verify project files against known-good copies before the next download to controllers.

5.3 Example Hunting Query

This Microsoft Defender for Endpoint query implements the core review logic and can be adapted to other EDR platforms. Run it across all Windows hosts, as the attacker's copy can run anywhere.

```
// Software Center started from a user profile, by a script host or installer, or below the fixed version
DeviceProcessEvents
| where FileName =~ "SiemensSoftwareCenter.exe"
| where FolderPath has @"\Users\"
    or InitiatingProcessFileName in~ ("powershell.exe", "cmd.exe", "mshta.exe", "msiexec.exe")
    or (isnotempty(ProcessVersionInfoProductVersion)
        and parse_version(ProcessVersionInfoProductVersion) < parse_version("4.0.9.8"))
| project Timestamp, DeviceName, FolderPath, ProcessVersionInfoProductVersion,
    InitiatingProcessFileName, InitiatingProcessCommandLine
```



A high-confidence detection after the upgrade. Once the estate is confirmed on 4.0.9.8 or later, any execution of SiemensSoftwareCenter.exe with a product version below 4.0.9.8, from any path, has no legitimate explanation. A single EDR rule on the binary's version, with the signature confirmed from file or image-load telemetry, turns the attacker's reliance on an old binary into a reliable detection.

5.4 Engineering Workstation Hardening

The campaign depends on running a signed binary from a user profile and on users executing pasted commands. These controls remove both conditions.

- **Execution control:** use WDAC or AppLocker to block programs and DLLs in AppData, Downloads and Temp, and require Siemens-signed Software Center at file version 4.0.9.8 or above. Publisher rules with a minimum version block the attacker's older copy despite its valid Siemens signature.
- **Command execution:** apply PowerShell Constrained Language Mode and script block logging, and remove the Run dialog by Group Policy on dedicated engineering hosts where acceptable.
- **Hygiene:** remove superseded Software Center installers from shares and engineering media, avoid administrative accounts for daily work, and health-check contractor laptops before plant connection.

Risk: CRITICAL HIGH MEDIUM TO VALIDATE **Status:** OPEN IN PROGRESS REMEDIATED

You may also directly check for potentially affected assets in **NST Assure** EA datasets.

How to check this in NST Assure. In NST Assure, go to Exposure Assessment and open the Technology Insights and Exploitation Intelligence datasets. Search for “WAGO”, “Moxa”, “ThingsPro”, “Industrial Edge”, “SIMATIC” or “VeloCloud” to find externally reachable OT and SD-WAN management services across your estate. These results support recommendation 4; CVE-2026-110936 itself affects internal hosts and cannot be confirmed from outside.

Sources: SOC Prime: CVE-2026-110936 | Daily Security Review | OpenCVE: CVE-2026-110936 | CISA ICS advisories, 20 October 2026 | The Register: CVE-2026-16812 | Canadian Centre for Cyber Security AV26-947

Based on public information as at 26 October 2026, for the recipient's internal use. Consult vendor advisories before changing operational systems.