contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

# Siemens Software Center exploited

**CVE-2026-110936 · on CISA's exploited list since 20 October 2026**

## Analysis Report

If you run Siemens Software Center, update it to V4.0.9.8 or later by 3 November 2026. Check the installed version first. If you do not run this product, you can stop reading.

| | | | |
|---|---|---|---|
| PREPARED BY | NamiQ | DATE | 1 November 2026 |
| FACTS AS OF | 1 November 2026 | VERSION | 1.0 |
| SEVERITY | **High: CVSS 4.0 8.4** | STATUS | On CISA's exploited list; due 3 November 2026 |

**NamiQ** © 2026 NamiQ. All rights reserved. This document is the property of NamiQ. It may be shared unaltered, with attribution.
Companion article: namiq.io/insights/siemens-software-center-cve-2026-110936

## The bottom line

> *If you run Siemens Software Center, update it to V4.0.9.8 or later by 3 November 2026. Check the installed version first. If you do not run this product, you can stop reading.*

## At a glance

| Fact | Detail |
|---|---|
| Product | Siemens Software Center (CVE-2026-110936) |
| Severity | High: 8.4 (CVSS 4.0) |
| CISA | On its exploited list since 20 October 2026. Deadline for US federal agencies: 3 November 2026. |
| Chance of exploitation (EPSS) | 0.01, the estimated chance in the next 30 days, as at 1 November 2026 |
| Ransomware use | Not recorded by CISA. That is not the same as none. |
| Fixed in | Siemens Software Center V4.0.9.8 or later (Siemens advisory, last updated 19 October 2026) |
| Who looks first | Anyone with Siemens Software Center installed. It downloads, installs and activates purchased Siemens software. Machines that other people can log in to matter most. |

## Does this apply to you?

**Answer in order. Stop at the first no.**

| Question | If no | If yes |
|---|---|---|
| Is Siemens Software Center installed on any machine you manage? | Nothing to do for this CVE. | Check the version (next question). |
| Is the installed version older than V4.0.9.8? | You are on the fixed release. Note the version in writing. | Update now, or restart the application so it updates itself. |
| Can anyone besides trusted administrators log in to that machine? | Risk is lower, but still update within CISA's window. | Treat it as the first machine to patch. |

## What it is

The record says the application loads DLL files from a search path that is not controlled. An attacker who is already logged in on the machine can place a crafted DLL in a searched folder. The code then

runs with the application's privileges.

## Why it matters

Our reading is that this flaw is not a way in from outside. It matters after an attacker has a foothold, because it turns a local login into code running with the application's privileges. The record needs a logged-in local attacker, and the vendor's v3.1 score is 6.7, so it can look minor. The advisory says Siemens knows of active exploitation, so a low score is not a reason to wait.

## What the vendor's advisory says

We read two pages on cert-portal.siemens.com and productcert.siemens.com. In short:

- Siemens advisory SSA-580366 lists one flaw, this one. It was first published on 15 October 2026 and last updated on 19 October 2026.
- The advisory scores it 6.7 under CVSS v3.1 and 8.4 under CVSS v4.0. The weakness is CWE-427, Uncontrolled Search Path Element.
- The vendor says to update to V4.0.9.8 or later. It says all existing versions auto-update on next startup.
- Version 1.2 of the advisory added a reference to a Siemens blog post on active exploitation and how to detect it.
- The advisory gives no workaround. It only repeats general advice to protect network access to devices.

## Things people will get wrong

- "It needs a login, so it is not urgent." The advisory says active exploitation is known. A local attacker's login is exactly the foothold this flaw builds on.
- "A score of 6.7 means it can wait." Siemens scores it 8.4 under CVSS v4.0 and 6.7 under v3.1. The two scoring versions disagree, and the advisory reports exploitation.
- "The software updates itself, so we are fine." The advisory says it updates on next startup. A machine where it has not been started may still be on an older version.

The wording includes conditions the score may not show: it needs privileges; the attacker must be logged in. Read the record before you decide it does not apply to you.

## How we would triage it

This is our judgement.

## Step 1: Find the versions you run

- List every machine with Siemens Software Center installed.
- Note the version on each. Anything before V4.0.9.8 is affected.

## Step 2: Limit who can log in

- Until patched, remove login rights from people who do not need them on affected machines. The attacker must already be logged in.

## Step 3: Update to V4.0.9.8 or later

- Start the application so it updates itself, or download the latest version from Siemens.
- Do this by 3 November 2026.

## Step 4: Confirm and check for signs of use

- Re-check the version after the update.
- Look for signs of use, using the detection guidance in the Siemens blog post the advisory refers to.

To close it, read the version from the product itself, not from an old inventory, and save the output with the date. If you cannot update today, write down who owns it, the new date, and what limits exposure until then.

## Send this to your IT provider

Copy it, change the names and dates, and send it. It is a draft for you to check, not a template tested with any provider.

> *Hello. Siemens Software Center has a flaw, CVE-2026-110936, in which a logged-in local user can run code through a planted DLL. Siemens advises updating to V4.0.9.8 or later, and CISA asks for action by 3 November 2026. Please tell us whether we run it, on which machines, and which version each has. Please update any older installation, then confirm the version and the fix in writing by 3 November 2026. If any machine cannot be updated by then, please tell us why and what you have done to limit who can log in to it. Thank you.*

## Signs it was used

An update closes the hole. It does not tell you whether someone used it first. CISA's required action points to its forensic triage requirements (BOD 26-04). Look for:

- Unexpected DLL files in folders the application searches, especially recently created ones.
- Software Center starting a process you do not recognise, or running when nobody started it.
- Whether the installed version is older than V4.0.9.8, as the earliest sign of exposure.

## The weakness behind it

The record classes this as CWE-427 (Uncontrolled Search Path Element).

## The sources, in their words

CISA's catalogue entry:

> *Siemens Software Center contains an uncontrolled search path element vulnerability that could allow an authenticated local attacker to place a specially crafted DLL in a directory that the application searches, leading to arbitrary code execution with the privileges of the affected application.*

The CVE record, published by Siemens on 15 October 2026:

> *A vulnerability has been identified in Siemens Software Center (All versions < V4.0.9.8). The affected application loads dynamic-link libraries (DLLs) from an uncontrolled search path. This could allow an authenticated local attacker to place a specially crafted DLL in a directory that the application searches, leading to arbitrary code execution with the privileges of the affected application.*

Versions of Siemens Software Center the record lists as affected:

- all versions before V4.0.9.8

The affected ranges end before V4.0.9.8. Those are the first versions the record does not list as affected; confirm them in the vendor's advisory.

CISA's required action:

> *Apply mitigations in accordance with vendor instructions, ensuring compliance with CISA's BOD 26-04 Prioritizing Security Updates Based on Risk (see URL in Notes) guidance and CISA's "Forensics Triage Requirements" (see URL in Notes).*

## What we do not know yet

- The sources do not say how attackers are using this flaw in practice.

- The sources do not say which Software Center versions the auto-update has already reached.
- The advisory gives no workaround for machines that cannot be updated at once.
- The advisory does not list which folders the application searches for DLLs.
- We have not tested this against any environment. Versions and scores are as the sources state them and as at 1 November 2026; the vendor's advisory wins where it differs.
- The sections headed "The bottom line", "Does this apply to you?", "What it is", "Why it matters", "Exposure by situation", "Things people will get wrong", "How we would triage it" and "Send this to your IT provider" are our interpretation of the sources, not a statement by CISA or the vendor.

## Appendix 1. Severity decoded

**CVE-2026-110936**: score 8.4, `CVSS:4.0/AV:L/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N` As the CVE record gives it. The record's own score can differ from the base score on the NVD record.

| Metric | Value | What it means here |
|---|---|---|
| Attack vector | Local | Needs an account or code already running on the machine. |
| Attack complexity | Low | No special conditions beyond the flaw itself. |
| Attack requirements | None | Works against a default deployment. |
| Privileges required | High | An administrator account is needed. |
| User interaction | None | No one has to do anything. |
| Vulnerable system: confidentiality | High | Total loss of confidentiality. |
| Vulnerable system: integrity | High | Total loss of integrity. |
| Vulnerable system: availability | High | Total loss of availability. |
| Subsequent systems: confidentiality | None | No data exposed. |
| Subsequent systems: integrity | None | Nothing can be altered. |
| Subsequent systems: availability | None | No effect on availability. |

## Appendix 2. Timeline

| Date | Event |
|---|---|
| 15 October 2026 | CVE record published by Siemens. |
| 20 October 2026 | CISA added it to its list of exploited vulnerabilities. |
| 3 November 2026 | CISA's deadline for US federal agencies. |

## Appendix 3. Exposure by situation

These priorities are our judgement from the attacker prerequisites in the sources. They are not vendor ratings.

| Your situation | Priority | Timeframe |
|---|---|---|
| A machine runs a version before V4.0.9.8 and several people can log in to it | High | Within CISA's window |

| | | |
|---|---|---|
| A single-user machine runs a version before V4.0.9.8 | High | Within CISA's window |
| The application is installed but has not been started for some time | Medium | Start it to trigger the update, this week |
| The machine already runs V4.0.9.8 or later | Low | Record the version, no further action |
| You do not run Siemens Software Center | None | None for this CVE |

## Appendix 4. Definition of done

- Every Siemens Software Center you run is listed, with its version.
- Each is outside the affected list, or the vendor's mitigation is in place.
- The version output or a screenshot is saved with the date.
- Logs for the weeks before the update were searched, and anything odd was written down.
- Anything not done has an owner and a date.

## Sources


- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- CVE record for CVE-2026-110936: https://www.cve.org/CVERecord?id=CVE-2026-110936
- FIRST: Exploit Prediction Scoring System: https://www.first.org/epss/
- Advisory or release notes read: cert-portal.siemens.com/productcert/html/ssa-580366.html: https://cert-portal.siemens.com/productcert/html/ssa-580366.html
- Advisory or release notes read: productcert.siemens.com/productcert/html/ssa-580366.html: https://productcert.siemens.com/productcert/html/ssa-580366.html