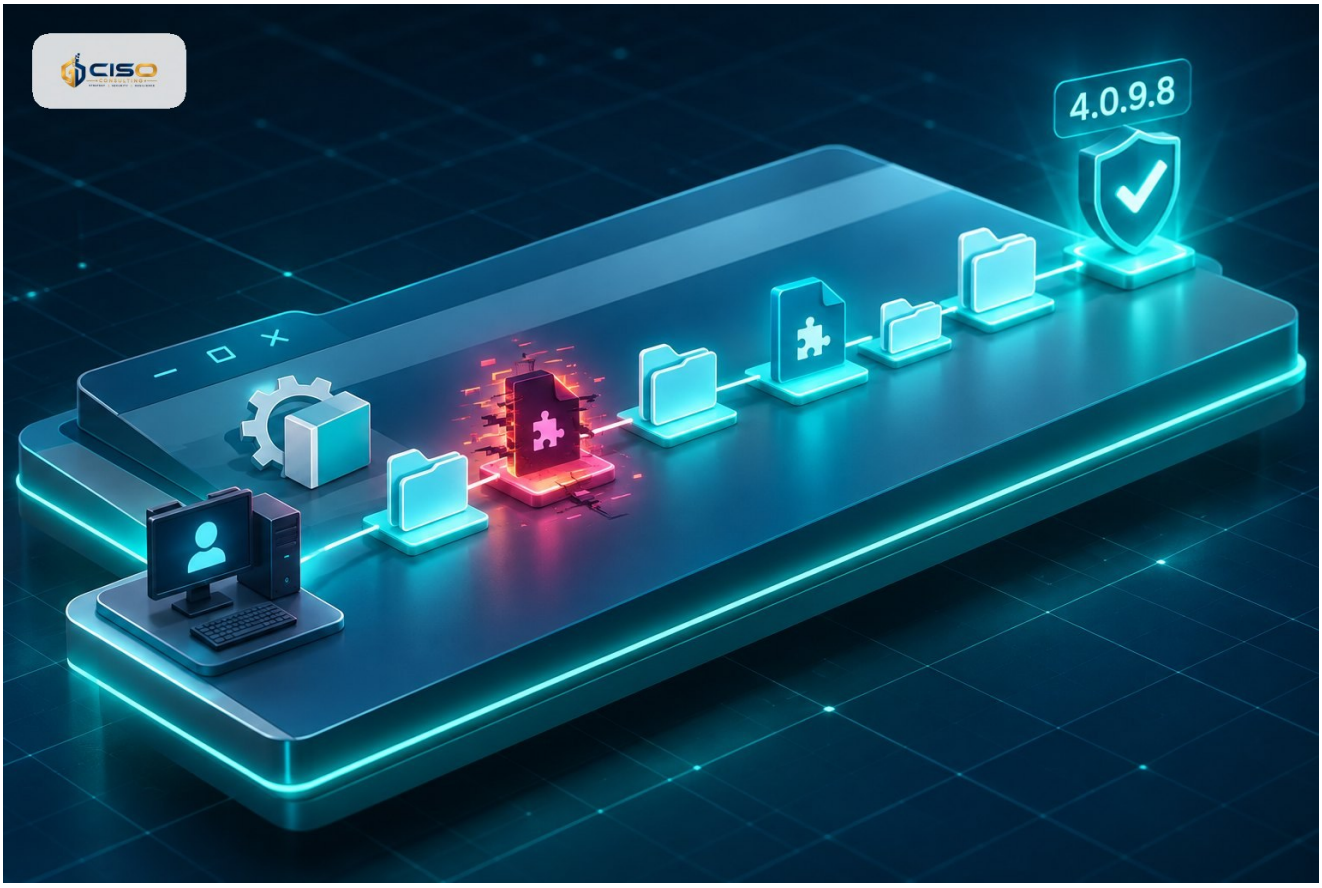
Siemens Software Center: DLL search-path flaw fixed in version 4.0.9.8



CISA reports a DLL search-path flaw (CVE-2026-110936, CVSS v3 6.7) in Siemens Software Center before 4.0.9.8. A local, authenticated attacker could run code. Siemens advises updating.

- CVE-2026-110936 affects Siemens Software Center versions earlier than 4.0.9.8.
- The application loads DLLs from an uncontrolled search path.
- An authenticated local attacker could achieve arbitrary code execution with the application's privileges.
- CVSS v3 score is 6.7; Siemens has released a fixed version and recommends updating.
- The advisory points to a blog post on known active exploitation and how to detect it.

What was reported

CISA has published an industrial control systems advisory on Siemens Software Center. The application loads dynamic-link libraries (DLLs) from an uncontrolled search path. An authenticated local attacker who can place a specially crafted DLL in a directory the application searches could cause arbitrary code to run with the privileges of the application.

The issue is tracked as **CVE-2026-110936** with a CVSS v3 score of 6.7. All versions earlier than 4.0.9.8 are affected. Siemens has released a new version and recommends updating to the latest one.

Why it matters

The advisory notes that the product is deployed worldwide and lists sectors including critical manufacturing, energy, healthcare, financial services, government services and transportation. It also refers readers to a blog post covering current known active exploitation and how to detect it, so teams should treat this as more than a routine patch.

Exploitation requires local access and authentication, which limits remote exposure, but the code would run with the application's privileges.

Recommended approach

Identify where Siemens Software Center is installed, confirm the version, and schedule the update to 4.0.9.8 or later. Review the CISA reference on detection and check affected hosts for unexpected DLLs in directories the application searches.

What to do now

1. Inventory all installations of Siemens Software Center and record their versions.
2. Update affected systems to version 4.0.9.8 or later following your change-management process.
3. Review the detection guidance referenced in the CISA advisory and check for unexpected DLLs in application search directories.
4. Restrict local and write access on hosts running the software to authorised users only.
5. Record the vulnerability and remediation in your vulnerability-management register for ECC and OTCC reporting where applicable.