

Siemens Fixes Software Center DLL Sideloaded Flaw Exploited in ClickFix Attacks



Siemens has fixed CVE-2026-110936, a high-severity DLL sideloading flaw in Siemens Software Center that it says was exploited in ClickFix attacks. Organisations using the software should apply the fix.

- Siemens has addressed a DLL sideloading vulnerability in Siemens Software Center.
- The flaw is tracked as CVE-2026-110936 with a CVSS v4 score of 8.4 (high).
- An attacker able to place a crafted DLL in a directory the application searches can run malicious code.
- The code runs with the same privileges as the application.
- Siemens said the flaw has been exploited in ClickFix attacks.

What was reported

Siemens has released a fix for a DLL sideloading vulnerability in Siemens Software Center. The company said the flaw has been exploited in ClickFix attacks. The issue is tracked as CVE-2026-110936 and carries a CVSS v4 score of 8.4, which places it in the high-severity range.

How the weakness works

DLL sideloading occurs when an application loads a library from a location an attacker can influence. In this case, an attacker could place a specially crafted DLL in a directory the application searches. The application would then execute the attacker's code with the same privileges the application itself holds.

The source ties the exploitation to ClickFix attacks, which generally depend on persuading a user to take an action themselves. The source excerpt does not give further detail on the campaigns, the affected versions or the fixed version, so those should be confirmed from the Siemens advisory.

Why it matters for regulated institutions

Engineering and industrial teams often install vendor tooling on workstations with elevated rights. A flaw that runs code at the application's privilege level can therefore matter more than its label suggests. Institutions should confirm whether Siemens Software Center is present in their estate and treat the update as a priority.

What to do now

1. Identify all systems where Siemens Software Center is installed.
2. Review the Siemens advisory for CVE-2026-110936 and apply the fix promptly.
3. Check the application directories on those systems for unexpected DLL files.
4. Restrict write access to application and search-path directories to administrators.
5. Remind staff not to paste or run commands from web pages or messages, as ClickFix relies on that.