GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu

Tel: (678) 33380

GOUVERNEMENT DE LA REPUBLIQUE DU VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE COMMUNICATION ET DE TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

21 October 2026

Advisory 364: Siemens Software Center DLL Side-Loading Vulnerability - Actively Exploited in ClickFix Attacks (CVE-2026-110936).

Release Date: 20th October 2026
Impact: HIGH
TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations and System/Network administrators that utilize the above product(s). This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-110936 is a DLL side-loading vulnerability (CWE-427, uncontrolled search path element) in Siemens Software Center. The application loads helper files from its own folder without checking them, so a malicious DLL placed next to the executable runs with the application's privileges.

What are the systems affected?

The following product is affected:

- Siemens Software Center, version 3.5.8.7 (the latest release at the time of the attacks) and, according to one analysis, all versions earlier than 4.0.9.8

Not affected / patched version:

- Siemens Software Center 4.0.9.8 or later
- Existing installations should update automatically at the next start. Administrators should verify the installed version rather than assume the update occurred

What does this mean?

Successful exploitation may allow attackers to:

- Run attacker-supplied code with the privileges of the logged-in user, hidden inside a genuine, validly signed Siemens program
- Install follow-on malware and establish command-and-control connections from the endpoint
- Evade detection that relies on file hashes or signatures of the Siemens executable

Mitigation process

CERTVU recommends the following:

1. Update Siemens Software Center
Update to version 4.0.9.8 or later on all endpoints and confirm the installed version. Download Siemens software only from official Siemens sources.

2. Block and search for the indicators

3. Detect by behavior, not by the Siemens file

Report suspected compromise to CERTVU.

Reference

1. https://productcert.siemens.com/news/2026/10/19/active-exploitation-of-cve-2026-110936-in-siemens-software-center
2. https://www.securityweek.com/siemens-software-center-vulnerability-exploited-in-clickfix-malware-attacks/
3. https://socprime.com/blog/cve-2026-110936-analysis/
4. https://www.helpnetsecurity.com/2026/10/20/exploitation-siemens-software-center-vulnerability-cve-2026-110936/
5. https://nvd.nist.gov/vuln/detail/CVE-2026-110936