Siemens Simcenter Femap: Out-of-Bounds Read Flaw in X_T File Handling (CVE-2026-64629)



CISA reports an out-of-bounds read flaw, CVE-2026-64629, in Siemens Simcenter Femap versions before V2606.0002. A crafted X_T file could crash the application or allow code execution. Siemens advises updating.

- Affected: Simcenter Femap versions earlier than V2606.0002.
- CVE-2026-64629 is an out-of-bounds read (CWE-125) triggered when parsing X_T files.
- CVSS v3.1 base score is 7.8 (High).
- Impact: application crash or code execution in the context of the current process.
- Fix: update to V2606.0002 or later.

What was reported

CISA has published an advisory on Siemens Simcenter Femap, an engineering application used in the critical manufacturing sector. The product contains an out-of-bounds read vulnerability, tracked as **CVE-2026-64629**, which appears when the application parses files in X_T format.

A specially crafted X_T file could cause the application to crash or allow an attacker to run code in the context of the current process. The issue is rated 7.8 (High) under CVSS v3.1 and is classified as CWE-125.

Who is affected

All Simcenter Femap versions earlier than V2606.0002 are listed as known affected. Siemens is headquartered in Germany, and the advisory notes worldwide deployment. The source does not mention any exploitation in the wild.

Recommended response

Siemens has released a fixed version and recommends updating to V2606.0002 or later. Organisations that run Femap, particularly in engineering, industrial or manufacturing environments, should identify installed versions and schedule the update through normal change control. Because the trigger is a file, it is also sensible to treat X_T files from unverified sources with caution until patching is complete.

What to do now

1. Inventory all Simcenter Femap installations and record their versions.
2. Update affected installations to V2606.0002 or later through change control.
3. Treat X_T files from unverified or external sources with caution until patched.
4. Restrict who can run Femap and open externally sourced files on engineering workstations.
5. Record the remediation in the vulnerability management register.