Siemens .NET Client Library for SIMATIC S7 Webserver API: two vulnerabilities, update advised



CISA reports two vulnerabilities in Siemens' .NET Client Library for the SIMATIC S7 Webserver API that could expose sensitive information or allow files to be written outside the download directory. Siemens advises updating.

- Two vulnerabilities: CVE-2026-85114 and CVE-2026-85115.
- Weakness types: path traversal and error messages that contain sensitive information.
- CVSS v3 score listed: 7.5.
- Affected: library versions below 3.3.61, and below 3.3.62 for the second entry.
- Siemens has released a new version and recommends updating to the latest.

CISA has published an advisory on Siemens' .NET Client Library for the SIMATIC S7 Webserver API. The library contains two vulnerabilities that could let an attacker obtain sensitive information or write arbitrary files outside the intended download directory.

What is affected

The advisory lists versions below 3.3.61 and below 3.3.62, with CVE-2026-85114 and CVE-2026-85115 referenced. The weaknesses are described as improper limitation of a pathname to a restricted directory (path traversal) and generation of error messages containing sensitive information. A CVSS v3 score of 7.5 is listed.

For CVE-2026-85114, the affected applications do not properly validate filenames received from remote servers during ticket downloads. An attacker able to manipulate the ticket response could therefore write files outside the intended location.

The advisory places the product in the Critical Manufacturing sector, deployed worldwide, from a vendor headquartered in Germany.

Recommended approach

Siemens has released a new version of the library and recommends updating to the latest release. Organizations that build or run in-house applications on this library, particularly in industrial or operational technology environments, should first establish whether they use it and which version is in place, then plan the update through normal change control.

The source does not report active exploitation, so a calm, prioritized approach is appropriate.

What to do now

1. Inventory applications and projects that use the .NET Client Library for SIMATIC S7 Webserver API and record versions.
2. Update affected applications to the latest library version released by Siemens.
3. Test the update in a non-production environment before deploying to OT-connected systems.
4. Review whether applications expose detailed error messages to untrusted users or logs.
5. Record the finding and remediation in vulnerability management and OT risk registers.