Siemens Mendix Studio Pro: MCP Server flaws allow remote access and CSRF attacks



CISA reports two vulnerabilities in the MCP Server of Siemens Mendix Studio Pro 11 (CVSS v3 8.8). Siemens has released fixed versions and advises updating to the latest release.

- Two vulnerabilities, CVE-2026-112136 and CVE-2026-112137, affect the MCP Server in Mendix Studio Pro.
- The weaknesses are binding to an unrestricted IP address and cross-site request forgery (CSRF).
- Affected: Mendix Studio Pro 11 from 11.15.0 up to below 11.16.0, and 11.12 from 11.12.6 up to below 11.12.7.
- Possible impact includes unauthorized data access, tool execution or system compromise.
- Siemens has released new versions and recommends updating to the latest.

CISA has published an advisory on Siemens Mendix Studio Pro covering two vulnerabilities in its MCP Server component. The vendor-assigned CVSS v3 score is 8.8.

What is affected

The first issue, CVE-2026-112136, concerns the MCP Server not properly restricting its HTTP listener to the loopback interface. This leaves it potentially reachable from remote systems. The second, CVE-2026-112137, is a cross-site request forgery weakness that could let an attacker trick a user's browser into sending unauthorized requests.

According to the advisory, an attacker with network access could interact with the server remotely, which could lead to unauthorized data access, tool execution or system compromise.

Affected versions are:

- Mendix Studio Pro 11: from 11.15.0 up to, but not including, 11.16.0
- Mendix Studio Pro 11.12: from 11.12.6 up to, but not including, 11.12.7

CISA lists the affected sectors as Critical Manufacturing and Energy, with worldwide deployment. Siemens is headquartered in Germany.

What to do

Siemens has released new versions of the affected products and recommends moving to the latest. Organizations that use Mendix Studio Pro, particularly those building applications for industrial or operational environments, should confirm which versions their developers run and plan the update through normal change control.

What to do now

1. Inventory Mendix Studio Pro installations and identify any in the affected version ranges.
2. Update to the latest Siemens release following your change-management process.
3. Check whether the MCP Server is reachable from other hosts and restrict network access to developer workstations where possible.
4. Remind developers to avoid browsing untrusted sites while Studio Pro is running until patched.
5. Record the exposure and remediation in your vulnerability management register.