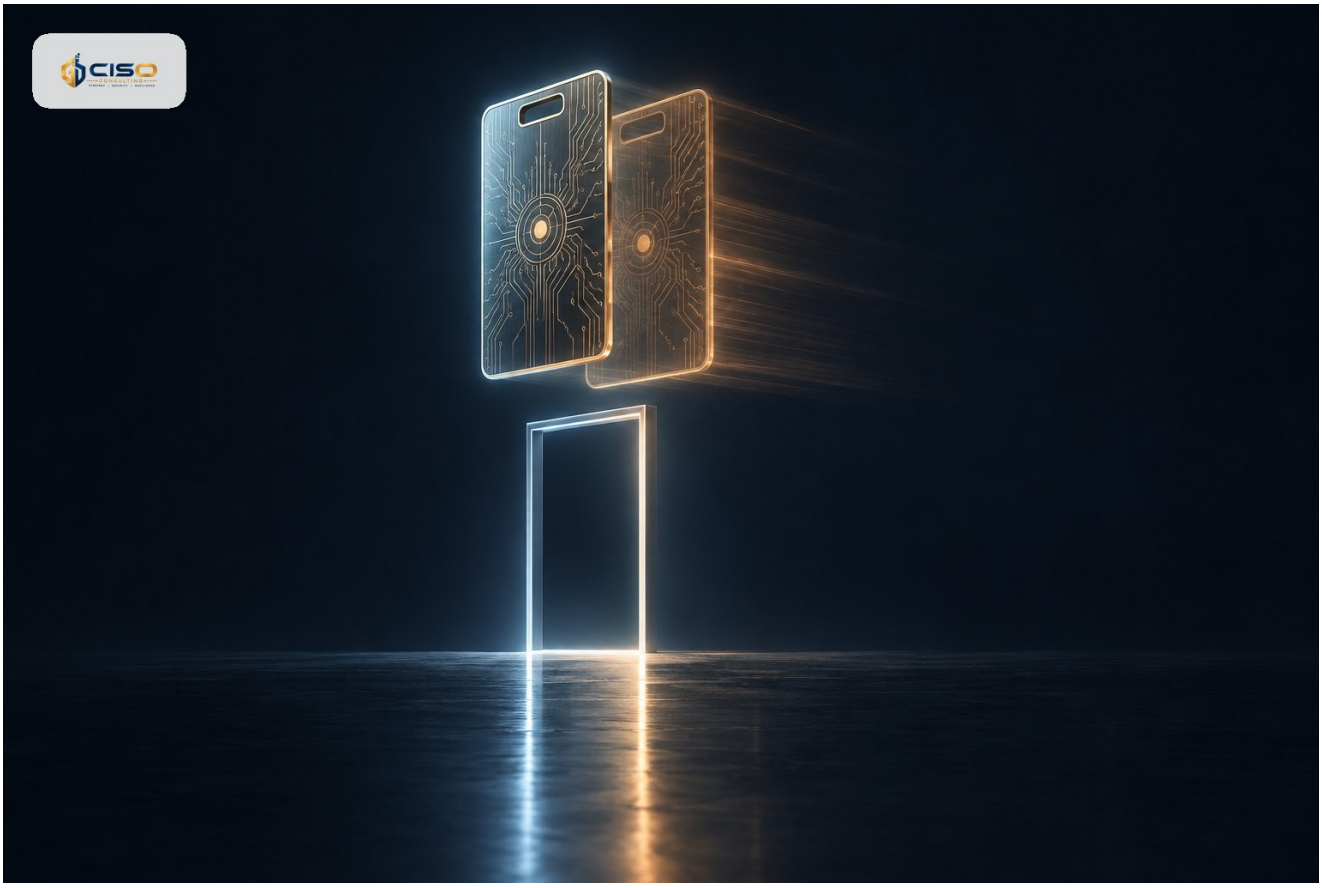
Siemens Mendix SAML Module: Authentication Bypass via Assertion Replay (CVE-2026-89209)



CISA reports a replay flaw in the Siemens Mendix SAML module that could let an unauthenticated remote attacker gain access through IdP-initiated sign-in. Siemens has released fixed versions.

- CVE-2026-89209 is an authentication bypass caused by weak protection against SAML assertion replay.
- It affects IdP-initiated authentication flows and can be exploited remotely without authentication.
- Affected: Mendix 10 and 11 compatible modules below 4.2.4, and Mendix 9 compatible modules below 3.6.29.
- The CVSS v3 score is 6.8.
- Siemens recommends updating to the latest versions.

CISA has published an advisory on an authentication bypass in the Siemens Mendix SAML module, tracked as CVE-2026-89209. The module does not adequately protect against replay of SAML assertions in flows initiated by the identity provider (IdP).

What is affected

An unauthenticated remote attacker who replays a valid SAML assertion could gain unauthorized access to the application. The affected versions are:

- Mendix SAML (Mendix 10 compatible): versions below 4.2.4
- Mendix SAML (Mendix 11 compatible): versions below 4.2.4
- Mendix SAML (Mendix 9 compatible): versions below 3.6.29

The advisory lists a CVSS v3 score of 6.8. It names Critical Manufacturing and Information Technology as the relevant sectors, with worldwide deployment. Siemens is headquartered in Germany.

What to do next

Siemens has released new versions and recommends updating to the latest ones. Organizations that build applications on Mendix and use the SAML module for single sign-on should first identify which applications include it and at which version. Updates should then be scheduled according to the exposure of each application, with internet-facing applications first.

The source does not describe active exploitation, so this is a prioritized patching task rather than an emergency. Teams should still confirm the fix in a test environment before release, and review authentication logs for unusual repeated sign-ins.

What to do now

1. Inventory Mendix applications that use the SAML module and record the module version in each.
2. Update to the latest Siemens-released versions, starting with internet-facing applications.
3. Test the update in a non-production environment before release.
4. Review authentication logs for repeated or unusual IdP-initiated sign-ins.
5. Record the vulnerability and remediation in the vulnerability management register.