Vulnerability Report: GO-2026-4337 standard library

Affects: crypto/tls | Published: Feb 05, 2026

During session resumption in crypto/tls, if the underlying Config has its ClientCAs or RootCAs fields mutated between the initial handshake and the resumed handshake, the resumed handshake may succeed when it should have failed. This may happen when a user calls Config.Clone and mutates the returned Config, or uses Config.GetConfigForClient. This can cause a client to resume a session with a server that it would not have resumed with during the initial handshake, or cause a server to resume a session with a client that it would not have resumed with during the initial handshake.

Affected Packages

Path	crypto/tls
Go Versions	before go1.24.13, from go1.25.0-0 before go1.25.7, from go1.26.0-rc.1 before go1.26.0-rc.3
Symbols	▶ 9 affected symbols

Aliases

CVE-2025-68121

References

https://groups.google.com/g/golang-announce/c/K09ubi9FQFk

https://go.dev/cl/737700

https://go.dev/issue/77217

https://vuln.go.dev/ID/GO-2026-4337.json

Credits

Coia Prant (github.com/rbqvq), Go Security Team

Feedback