[security] Go 1.25.7 and Go 1.24.13 are released

anno...@golang.org
to golan...@googlegroups.com

Hello gophers,

We have just released Go versions 1.25.7 and 1.24.13, minor point releases.

These releases include 2 security fixes following the security policy:

- cmd/cgo: remove user-content from doc strings in cgo ASTs

  A discrepancy between how Go and C/C++ comments were parsed allowed for code smuggling into the resulting cgo binary.

  To prevent this behavior, the cgo compiler will no longer parse user-provided doc comments.

  Thank you to RyotaK (https://ryotak.net) of GMO Flatt Security Inc. for reporting this issue.

  This is CVE-2025-61732 and https://go.dev/issue/76697.

- crypto/tls: unexpected session resumption when using Config.GetConfigForClient

  Config.GetConfigForClient is documented to use the original Config's session ticket keys unless explicitly overridden. This can cause unexpected behavior if the returned Config modifies authentication parameters, like ClientCAs: a connection initially established with the parent (or a sibling) Config can be resumed, bypassing the modified authentication requirements.

  If ClientAuth is VerifyClientCertIfGiven or RequireAndVerifyClientCert (on the server) or InsecureSkipVerify is false (on the client), crypto/tls now checks that the root of the previously-verified chain is still in ClientCAs/RootCAs when resuming a connection.

  Go 1.26 Release Candidate 2, Go 1.25.6, and Go 1.24.12 had fixed a similar issue related to session ticket keys being implicitly shared by Config.Clone. Since this fix is broader, the Config.Clone behavior change has been reverted.

  Note that VerifyPeerCertificate still behaves as documented: it does not apply to resumed connections. Applications that use Config.GetConfigForClient or Config.Clone and do not wish to blindly resume connections established with the original Config must use VerifyConnection instead (or SetSessionTicketKeys or SessionTicketsDisabled).

  Thanks to Coia Prant (github.com/rbqvq) for reporting this issue.

  This updates CVE-2025-68121 and Go issue https://go.dev/issue/77217.

View the release notes for more information:
https://go.dev/doc/devel/release#go1.25.7

You can download binary and source distributions from the Go website:
https://go.dev/dl/

To compile from source using a Git clone, update to the release with `git checkout go1.25.7` and build as usual.

Thanks to everyone who contributed to the releases.

Cheers,
Michael and Dmitri for the Go team