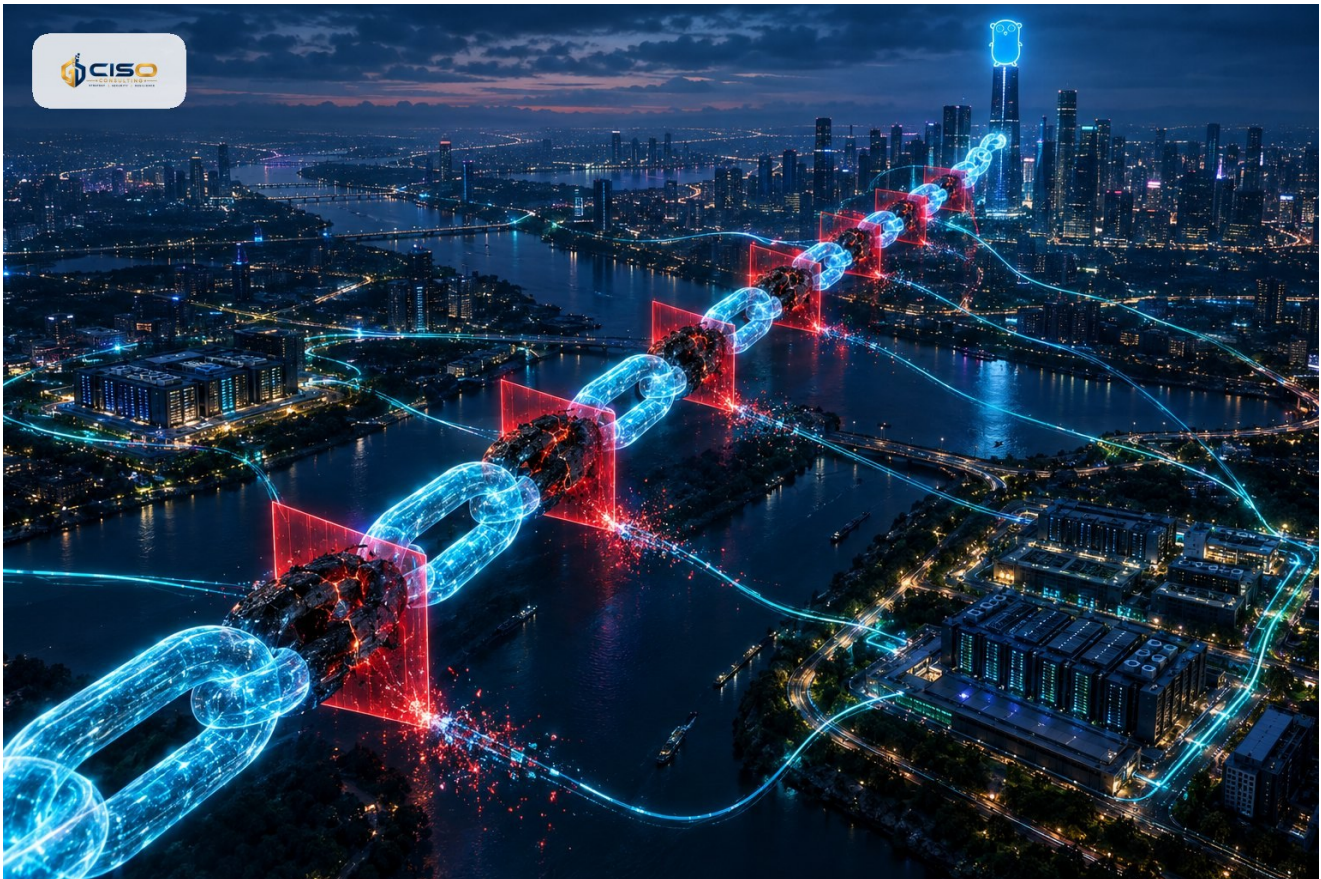


Go 1.27.3 and 1.26.10 block eight intermediate CA keys in certificate verification



Go's emergency releases 1.27.3 and 1.26.10, issued on October 20, now reject certificate chains passing through eight intermediate CA keys. Applications built with them will refuse connections to services using certificates issued under those keys.

- Go 1.27.3 and Go 1.26.10 were released on October 20 as emergency updates.
- The certificate verifier now rejects any chain that passes through one of eight intermediate CA keys.
- Programs built on the new releases will refuse connections to sites and services whose certificates were issued under those keys.
- According to the source, the keys belong to a single certificate authority, and the security concerns behind the block were not disclosed.

The Go team has released Go 1.27.3 and Go 1.26.10 as emergency updates. In both versions, Go's certificate verifier rejects any certificate chain that passes through one of eight intermediate certificate authority keys.

What changes for applications

Programs built with the new releases will refuse connections to sites and services whose certificates were issued under the blocked keys. The effect is therefore on the client side: a Go application rebuilt on the patched toolchain may suddenly fail to connect to a dependency that was working before.

The source indicates that the eight keys belong to one certificate authority. The security concerns behind the decision have not been disclosed, so there is no public detail to assess beyond the block itself.

How to approach it

The practical risk for most organisations is availability rather than a new vulnerability. Teams that build Go services, internal tools or agents should expect that upgrading may expose connection failures towards endpoints using certificates from the affected authority. Testing before production rollout will show whether any such dependencies exist.

Because the source does not name the certificate authority in the excerpt available, teams should consult the official Go release notes for the exact list of blocked keys before deciding on next steps.

What to do now

1. Inventory internal and third-party applications built with Go and identify which toolchain versions they use.
2. Review the official Go 1.27.3 and 1.26.10 release notes for the exact list of blocked intermediate keys.
3. Test rebuilt applications in a non-production environment against the external and internal endpoints they depend on.
4. Check the certificate chains of critical dependencies for any path through the blocked keys.
5. Plan the rollout through change management, with a rollback path in case of unexpected connection failures.