New issue

crypto/x509: excluded DNS constraints not properly applied to wildcard domains #78332

Closed

Labels NeedsFix Security release-blocker vulncheck or vulndb

Milestone Go1.27

neild opened last month · edited by dr2chase Edits Contributor

When verifying a certificate chain containing excluded DNS constraints, these constraints are not correctly applied to wildcard DNS SANs which use a different case than the constraint.

For example, if a certificate contains the DNS name "*.example.com" and the excluded DNS name "EXAMPLE.COM", the constraint will not be applied.

This only affects validation of otherwise trusted certificate chains, issued by a root CA in the VerifyOptions.Roots CertPool, or in the system certificate pool.

This issue only affects Go 1.26.

Thank you to Riyas from Saintgits College of Engineering, k1rnt, **@1seal** for reporting this issue.

This is CVE-2026-33810 and Go issue https://go.dev/issue/78332.

This is a PRIVATE issue for CVE-2026-33810, tracked in http://b/491458235 and fixed by https://go-internal-review.git.corp.google.com/c/go/+/3860.

neild added this to the Go1.27 milestone last month

neild added Security release-blocker last month

gabyhelp added vulncheck or vuln... last month

dmitshur added NeedsFix last month

dmitshur last month Member

CC @golang/security, @golang/release.

neild 3 weeks ago Contributor Author

@**gopherbot** please backport to go1.26.

gopherbot 3 weeks ago Contributor

Backport issue(s) opened: #78418 (for 1.26).

Remember to create the cherry-pick CL(s) as soon as the patch is submitted to master, according to https://go.dev/wiki/MinorReleases.

gopherbot mentioned this 3 weeks ago

security: fix CVE-2026-33810 [1.26 backport] #78418

gopherbot 2 weeks ago Contributor

Change https://go.dev/cl/763544 mentions this issue: `[release-branch.go1.26] crypto/x509: fix wildcard constraint map case sensitivity`

gopherbot added a commit that references this issue 2 weeks ago

`[release-branch.go1.26] crypto/x509: fix wildcard constraint map case.` ··· ceb4da6

dr2chase changed the title ~~security: fix CVE-2026-33810~~ crypto/x509: excluded DNS constraints not properly applied to wildcard domains 2 weeks ago

gopherbot 2 weeks ago Contributor

Change https://go.dev/cl/763763 mentions this issue: `crypto/x509: fix wildcard constraint map case sensitivity`

gopherbot closed this as completed in 4978c20 2 weeks ago

pull added a commit that references this issue 2 weeks ago

`crypto/x509: fix wildcard constraint map case sensitivity` ··· 4978c20

thomasmaas mentioned this last week

Upgrade Go to 1.25.9 across all repos Kuadrant/kuadrant-operator#1886

coderabbitai mentioned this 24 minutes ago

Flag fleetdm/fleetctl vulnerabilities fleetdm/fleet#43785

Metadata

Assignees

No one assigned

Labels

NeedsFix Security release-blocker vulncheck or vulndb

Type

No type

Projects

No projects

Milestone

Go1.27

No due date

Relationships

None yet

Development

No branches or pull requests

Participants