Unexpected session resumption in crypto/tls

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2025-68121
State	PUBLISHED
Assigner	Go
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-02-05 18:16:10 UTC
Updated	2026-04-29 14:16:16 UTC
Description	During session resumption in crypto/tls, if the underlying Config has its ClientCAs or RootCAs fields mutated between the ir

Risk And Classification

Primary CVSS: v3.1 10 CRITICAL from nvd@nist.gov

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Problem Types: CWE-295 | CWE-295: Improper Certificate Validation | CWE-295 CWE-295 Improper Certificate Validation

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	10	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
3.1	ADP	DECLARED	9.1	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	9.1	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Changed

Confidentiality

High

ntegrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Golang	Go	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Go Standard Library	Crypto/tls	affected 1.24.13 semver	Not specified
CNA	Go Standard Library	Crypto/tls	affected 1.25.0-0 1.25.7 semver	Not specified
CNA	Go Standard Library	Crypto/tls	affected 1.26.0-rc.1 1.26.0-rc.3 semver	Not specified

References

Reference	Source	Link	Tags
pkg.go.dev/vuln/GO-2026-4337	security@golang.org	pkg.go.dev	Vendor Advisory
groups.google.com/g/golang-announce/c/K09ubi9FQFk	security@golang.org	groups.google.com	Mailing List, Third Party Advisory
go.dev/issue/77217	security@golang.org	go.dev	Exploit, Issue Tracking
go.dev/cl/737700	security@golang.org	go.dev	Patch
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

Discovery Credit

CNA: Coia Prant (github.com/rbqvq) (en)

CNA: Go Security Team (en)

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**