Panic in name constraint checking for malformed certificates in crypto/x509

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

Summary

CVE	CVE-2026-27138
State	PUBLISHED
Assigner	Go
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-06 22:16:00 UTC
Updated	2026-04-21 14:39:28 UTC
Description	Certificate verification can panic when a certificate in the chain has an empty DNS name and another certificate in the chair

Risk And Classification

Primary CVSS: v3.1 5.9 MEDIUM from ADP

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

EPSS: 0.000210000 probability, percentile 0.058940000 (date 2026-04-21)

Problem Types: CWE-295 | CWE-1285: Improper Validation of Specified Index, Position, or Offset in Input

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	5.9	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	5.9	MEDIUM	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

ntegrity

None

Availability

High

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Golang	Go	1.26.0	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Go Standard Library	Crypto/x509	affected 1.26.0-0 1.26.1 semver	Not specified

References

Reference	Source	Link	Tags
pkg.go.dev/vuln/GO-2026-4600	security@golang.org	pkg.go.dev	Vendor Advisory
groups.google.com/g/golang-announce/c/EdhZqrQ98hk	security@golang.org	groups.google.com	Release Notes
go.dev/cl/752183	security@golang.org	go.dev	Mailing List
go.dev/issue/77953	security@golang.org	go.dev	Issue Tracking
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: Jakub Ciolek (en)

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

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