



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

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

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

## 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

Integrity

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	<a href="https://pkg.go.dev">pkg.go.dev</a>	Vendor Advisory
groups.google.com/g/golang-announce/c/EdhZqrQ98hk	security@golang.org	<a href="https://groups.google.com">groups.google.com</a>	Release Notes
go.dev/cl/752183	security@golang.org	<a href="https://go.dev">go.dev</a>	Mailing List
go.dev/issue/77953	security@golang.org	<a href="https://go.dev">go.dev</a>	Issue Tracking
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	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 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/cve).

Free CVE JSON API [cve.report/api](https://cve.report/api)

