Case-sensitive excludedSubtrees name constraints cause Auth Bypass in crypto/x509

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

Summary

CVE	CVE-2026-33810
State	PUBLISHED
Assigner	Go
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-08 02:16:03 UTC
Updated	2026-04-17 20:41:13 UTC
Description	When verifying a certificate chain containing excluded DNS constraints, these constraints are not correctly applied to wildca

Risk And Classification

Primary CVSS: v3.1 8.2 HIGH from nvd@nist.gov

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

EPSS: 0.000110000 probability, percentile 0.012220000 (date 2026-04-17)

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

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	8.2	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N
3.1	ADP	DECLARED	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

ntegrity

Low

Availability

None

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

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/x509	affected 1.26.0-0 1.26.2 semver	Not specified

References

Reference	Source	Link	Tags
pkg.go.dev/vuln/GO-2026-4866	security@golang.org	pkg.go.dev	Vendor Advisory
groups.google.com/g/golang-announce/c/0uYbvbPZRWU	security@golang.org	groups.google.com	Release Notes, Mailing List
go.dev/issue/78332	security@golang.org	go.dev	Issue Tracking
go.dev/cl/763763	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: Riyas from Saintgits College of Engineering (en)

CNA: k1rnt (en)

CNA: @1seal (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 registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

Free CVE JSON API cve.report/api

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