Incorrect parsing of IPv6 host literals in net/url

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

Summary

CVE	CVE-2026-25679
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 14:43:03 UTC
Description	url.Parse insufficiently validated the host/authority component and accepted some invalid URLs.

Risk And Classification

Primary CVSS: v3.1 7.5 HIGH from ADP

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

EPSS: 0.000510000 probability, percentile 0.158810000 (date 2026-04-21)

Problem Types: CWE-425 | CWE-1286: Improper Validation of Syntactic Correctness of Input

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
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:N/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

CVSS:3.1/AV:N/AC:L/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	All	All	All	All
Application	Golang	Go	1.26.0	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Go Standard Library	Net/url	affected 1.25.8 semver	Not specified
CNA	Go Standard Library	Net/url	affected 1.26.0-0 1.26.1 semver	Not specified

References

Reference	Source	Link	Tags
go.dev/issue/77578	security@golang.org	go.dev	Issue Tracking
pkg.go.dev/vuln/GO-2026-4601	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/752180	security@golang.org	go.dev	Mailing List
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: Masaki Hara (https://github.com/qnighy) of Wantedly (en)

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

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