HTTP Proxy bypass using IPv6 Zone IDs in golang.org/x/net

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

Summary

CVE	CVE-2025-22870
State	PUBLISHED
Assigner	Go
Source Priority	CVE Program / NVD first with legacy fallback
Published	2025-03-12 19:15:38 UTC
Updated	2026-04-16 23:16:32 UTC
Description	Matching of hosts against proxy patterns can improperly treat an IPv6 zone ID as a hostname component. For example, wh

Risk And Classification

Primary CVSS: v3.1 4.4 MEDIUM from ADP

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

EPSS: 0.000310000 probability, percentile 0.086440000 (date 2026-04-16)

Problem Types: CWE-115 | CWE-115 Misinterpretation of Input | CWE-115 CWE-115 Misinterpretation of Input

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	4.4	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:L
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	4.4	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:L

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

Low

ntegrity

None

Availability

Low

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Go Standard Library	Net/http	affected 1.23.7 semver	Not specified
CNA	Go Standard Library	Net/http	affected 1.24.0-0 1.24.1 semver	Not specified
CNA	Golang.orgxnet	Golang.org/x/net/http/httpproxy	affected 0.36.0 semver	Not specified
CNA	Golang.orgxnet	Golang.org/x/net/proxy	affected 0.36.0 semver	Not specified

References

Reference	Source	Link
groups.google.com/g/golang-announce/c/4t3lzH3l0el/m/b42ImqrBAQAJ	security@golang.org	groups.google.com
security.netapp.com/advisory/ntap-20250509-0007	af854a3a-2127-422b-91ae-364da2661108	security.netapp.com
www.openwall.com/lists/oss-security/2025/03/07/2	af854a3a-2127-422b-91ae-364da2661108	www.openwall.com
go.dev/cl/654697	security@golang.org	go.dev
go.dev/issue/71984	security@golang.org	go.dev
pkg.go.dev/vuln/GO-2025-3503	security@golang.org	pkg.go.dev
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

CNA: Juho Forsén of Mattermost (en)

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

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