



# HTTP Proxy bypass using IPv6 Zone IDs in [golang.org/x/net](https://golang.org/x/net)

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

## Summary

<b>CVE</b>	CVE-2025-22870
<b>State</b>	PUBLISHED
<b>Assigner</b>	Go
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2025-03-12 19:15:38 UTC
<b>Updated</b>	2026-04-16 23:16:32 UTC
<b>Description</b>	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

Integrity

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	<a href="#">Go Standard Library</a>	<a href="#">Net/http</a>	affected 1.23.7 semver	Not specified
CNA	<a href="#">Go Standard Library</a>	<a href="#">Net/http</a>	affected 1.24.0-0 1.24.1 semver	Not specified
CNA	<a href="#">Golang.orgxnet</a>	<a href="#">Golang.org/x/net/http/httpproxy</a>	affected 0.36.0 semver	Not specified
CNA	<a href="#">Golang.orgxnet</a>	<a href="#">Golang.org/x/net/proxy</a>	affected 0.36.0 semver	Not specified

### References

Reference	Source	Link
<a href="https://groups.google.com/g/golang-announce/c/4t3lzH3l0el/m/b42lmqrBAQAJ">groups.google.com/g/golang-announce/c/4t3lzH3l0el/m/b42lmqrBAQAJ</a>	<a href="mailto:security@golang.org">security@golang.org</a>	<a href="https://groups.google.com">groups.google.com</a>
<a href="https://security.netapp.com/advisory/ntap-20250509-0007">security.netapp.com/advisory/ntap-20250509-0007</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="https://security.netapp.com">security.netapp.com</a>
<a href="https://www.openwall.com/lists/oss-security/2025/03/07/2">www.openwall.com/lists/oss-security/2025/03/07/2</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="https://www.openwall.com">www.openwall.com</a>
<a href="https://go.dev/cl/654697">go.dev/cl/654697</a>	<a href="mailto:security@golang.org">security@golang.org</a>	<a href="https://go.dev">go.dev</a>
<a href="https://go.dev/issue/71984">go.dev/issue/71984</a>	<a href="mailto:security@golang.org">security@golang.org</a>	<a href="https://go.dev">go.dev</a>
<a href="https://pkg.go.dev/vuln/GO-2025-3503">pkg.go.dev/vuln/GO-2025-3503</a>	<a href="mailto:security@golang.org">security@golang.org</a>	<a href="https://pkg.go.dev">pkg.go.dev</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

### Vendor Comments And Credit

#### Discovery Credit

**CNA:** Juho Forsén of Mattermost (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](#) 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](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)