



# TOCTOU permits root escape on Linux via Root.Chmod in os in internal/syscall/unix

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

## Summary

<b>CVE</b>	CVE-2026-32282
<b>State</b>	PUBLISHED
<b>Assigner</b>	Go
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-04-08 02:16:03 UTC
<b>Updated</b>	2026-04-16 19:15:39 UTC
<b>Description</b>	On Linux, if the target of Root.Chmod is replaced with a symlink while the chmod operation is in progress, Chmod can oper

## Risk And Classification

**Primary CVSS:** v3.1 6.4 MEDIUM from nvd@nist.gov

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

**EPSS:** 0.000080000 probability, percentile 0.007730000 (date 2026-04-15)

**Problem Types:** CWE-59 | CWE-61: UNIX Symbolic Link (Symlink) Following

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	6.4	MEDIUM	CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H
3.1	ADP	DECLARED	6.4	MEDIUM	CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	6.4	MEDIUM	CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H

## CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

High

Privileges Required

High

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

### 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	Internal/syscall/unix	affected 1.25.9 semver	linux
CNA	Go Standard Library	Internal/syscall/unix	affected 1.26.0-0 1.26.2 semver	linux

### References

Reference	Source	Link	Tags
pkg.go.dev/vuln/GO-2026-4864	security@golang.org	pkg.go.dev	Vendor Advisory
go.dev/issue/78293	security@golang.org	go.dev	Issue Tracking
groups.google.com/g/golang-announce/c/0uYbvbPZRWU	security@golang.org	groups.google.com	Release Notes, Mailing List
go.dev/cl/763761	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:** Uuganbayar Lkhamsuren (<https://github.com/uug4na>) (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)