



# FileInfo can escape from a Root in os

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

## Summary

<b>CVE</b>	CVE-2026-27139
<b>State</b>	PUBLISHED
<b>Assigner</b>	Go
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-03-06 22:16:01 UTC
<b>Updated</b>	2026-04-21 14:32:36 UTC
<b>Description</b>	On Unix platforms, when listing the contents of a directory using File.ReadDir or File.Readdir the returned FileInfo could ref

## Risk And Classification

**Primary CVSS:** v3.1 2.5 LOW from ADP

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

**EPSS:** 0.000080000 probability, percentile 0.007160000 (date 2026-04-21)

**Problem Types:** CWE-22 | CWE-363: Race Condition Enabling Link Following

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	2.5	LOW	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	2.5	LOW	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N

## CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

High

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

Low

Integrity

None

None

Availability

None

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

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Golang</a>	<a href="#">Go</a>	All	All	All	All
Application	<a href="#">Golang</a>	<a href="#">Go</a>	1.26.0	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	<a href="#">Go Standard Library</a>	<a href="#">Os</a>	affected 1.25.8 semver	Not specified
CNA	<a href="#">Go Standard Library</a>	<a href="#">Os</a>	affected 1.26.0-0 1.26.1 semver	Not specified

### References

Reference	Source	Link	Tags
<a href="#">pkg.go.dev/vuln/GO-2026-4602</a>	<a href="mailto:security@golang.org">security@golang.org</a>	<a href="#">pkg.go.dev</a>	Vendor Advisory
<a href="#">groups.google.com/g/golang-announce/c/EdhZqrQ98hk</a>	<a href="mailto:security@golang.org">security@golang.org</a>	<a href="#">groups.google.com</a>	Release Notes
<a href="#">go.dev/cl/749480</a>	<a href="mailto:security@golang.org">security@golang.org</a>	<a href="#">go.dev</a>	Mailing List
<a href="#">go.dev/issue/77827</a>	<a href="mailto:security@golang.org">security@golang.org</a>	<a href="#">go.dev</a>	Issue Tracking
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>	canonical, analysis

### Vendor Comments And Credit

Discovery Credit

**CNA:** Miloslav Trmač of Red Hat (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](#)

