



[Vulnerability Database](#) > [All Reports](#) > [GO-2026-4815](#)

Vulnerability Report: GO-2026-4815

Affects: [golang.org/x/image](#) | Published: Mar 25, 2026

A maliciously crafted TIFF file can cause image decoding to attempt to allocate up 4GiB of memory, causing either excessive resource consumption or an out-of-memory error.

Affected Packages

Path [golang.org/x/image/tiff](#)
Go Versions before v0.38.0
Symbols [Decode](#)
[DecodeConfig](#)

Aliases

[CVE-2026-33809](#)

References

<https://go.dev/cl/757660>

<https://go.dev/issue/78267>

<https://vuln.go.dev/ID/GO-2026-4815.json>

Feedback

See anything missing or incorrect? [Suggest an edit to this report.](#)

[Why Go](#)

[Get Started](#)

[Packages](#)

[About](#)

go.dev uses cookies from Google to deliver and enhance the quality of its services and to analyze traffic. [Learn more.](#)

Okay

[Case Studies](#)

[Tour](#)

[Sub-repositories](#)

[Blog](#)

[Stack Overflow](#)

[About Go Packages](#)

[Issue Tracker](#)

[Help](#)

[Release Notes](#)

[Brand Guidelines](#)

[Code of Conduct](#)

Connect

[Twitter](#)

[GitHub](#)

[Slack](#)

[r/golang](#)

[Meetup](#)

[Golang Weekly](#)

Copyright

[Terms of Service](#)

[Privacy Policy](#)

[Report an Issue](#)

 [Theme Toggle](#)

 [Shortcuts Modal](#)



Google

go.dev uses cookies from Google to deliver and enhance the quality of its services and to analyze traffic. [Learn more.](#)