



[Vulnerability Database](#) > [All Reports](#) > [GO-2024-2660](#)

Vulnerability Report: GO-2024-2660

Affects: [github.com/golang-fips/openssl/v2](#), [github.com/microsoft/go-crypto-openssl](#) |

Published: Mar 27, 2024 | Modified: May 20, 2024

Using crafted public RSA keys can cause a small memory leak when encrypting and verifying payloads. This can be gradually leveraged into a denial of service attack.

Affected Packages

Path [github.com/golang-fips/openssl/v2](#)

Go before v2.0.1

Versions

Symbols ▶ 15 affected symbols

Path [github.com/microsoft/go-crypto-openssl/openssl](#)

Go before v0.2.9

Versions

Symbols ▶ 14 affected symbols

Aliases

[CVE-2024-1394](#)

[GHSA-78hx-gp6g-7mj6](#)

References

<https://github.com/golang-fips/openssl/commit/85d31d0d257ce842c8a1e63c4d230ae850348136>

<https://github.com/microsoft/go-crypto-openssl/commit/104fe7f6912788d2ad44602f77a0a0a62f1f259f>

<https://vuln.go.dev/ID/GO-2024-2660.json>

Credits

@qmuntal and @r3kumar

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

Okay

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

Why Go

[Use Cases](#)

[Case Studies](#)

Get Started

[Playground](#)

[Tour](#)

[Stack Overflow](#)

[Help](#)

Packages

[Standard Library](#)

[Sub-repositories](#)

[About Go Packages](#)

About

[Download](#)

[Blog](#)

[Issue Tracker](#)

[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](#)



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