



# Missing bound checks can lead to memory corruption in safe Go in cmd/compile

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

## Summary

<b>CVE</b>	CVE-2026-27143
<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 19:20:02 UTC
<b>Description</b>	Arithmetic over induction variables in loops were not correctly checked for underflow or overflow. As a result, the compiler v

## Risk And Classification

**Primary CVSS:** v3.1 9.8 CRITICAL from nvd@nist.gov

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

**EPSS:** 0.000240000 probability, percentile 0.066180000 (date 2026-04-15)

**Problem Types:** NVD-CWE-Other | CWE-190: Integer Overflow or Wraparound

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	ADP	DECLARED	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/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 Toolchain	Cmd/compile	affected 1.25.9 semver	Not specified
CNA	Go Toolchain	Cmd/compile	affected 1.26.0-0 1.26.2 semver	Not specified

#### References

Reference	Source	Link	Tags
go.dev/issue/78333	security@golang.org	go.dev	Issue Tracking
pkg.go.dev/vuln/GO-2026-4868	security@golang.org	pkg.go.dev	Vendor Advisory
go.dev/cl/763765	security@golang.org	go.dev	Patch
groups.google.com/g/golang-announce/c/0uYbvbPZRWU	security@golang.org	groups.google.com	Release Notes, Mailing List
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:** Jakub Ciolek - <https://ciolek.dev/> (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)