



# GoBGP: Panic in AdjRib.Update via malformed BGP Update message (Nil Pointer Dereference)

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

## Summary

<b>CVE</b>	CVE-2026-42285
<b>State</b>	PUBLISHED
<b>Assigner</b>	GitHub_M
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-07 12:16:18 UTC
<b>Updated</b>	2026-05-11 15:22:48 UTC
<b>Description</b>	GoBGP is an open source Border Gateway Protocol (BGP) implementation in the Go Programming Language. In version 4.

## Risk And Classification

**Primary CVSS:** v3.1 7.5 HIGH from security-advisories@github.com

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

**EPSS:** 0.001340000 probability, percentile 0.327650000 (date 2026-05-12)

**Problem Types:** CWE-476 | CWE-476 CWE-476: NULL Pointer Dereference

Version	Source	Type	Score	Severity	Vector
3.1	security-advisories@github.com	Secondary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
3.1	CNA	DECLARED	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

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

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Osrg	Gobgp	4.4.0	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Osrg	Gobgp	affected = 4.4.0	Not specified

### References

Reference	Source	Link	Tags
github.com/osrg/gobgp/releases/tag/v4.5.0	security-advisories@github.com	github.com	Product, Rel
github.com/osrg/gobgp/security/advisories/GHSA-p3w2-64xm-833j	134c704f-9b21-4f2e-91b3-4a467353bcc0	github.com	Exploit, Venc
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ar

No vendor comments have been submitted for this CVE.

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)