



CVE-2023-26125

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

Summary

CVE	CVE-2023-26125
State	PUBLIC
Assigner	report@snyk.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-05-04 05:15:00 UTC
Updated	2023-11-07 04:09:00 UTC
Description	Versions of the package github.com/gin-gonic/gin before 1.9.0 are vulnerable to Improper Input Validation by allowing an at

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gin-gonic	Gin	All	All	All	All

References

Reference	Source	Link	Tags
Release v1.9.0 · gin-gonic/gin · GitHub	MISC	github.com	
Fix #3500 Add escape logic for header by t0rchwo0d · Pull Request #3503 · gin-gonic/gin · GitHub	MISC	github.com	
Add escape logic for header by t0rchwo0d · Pull Request #3500 · gin-gonic/gin · GitHub	MISC	github.com	
Fix #3500 Add escape logic for header · t0rchwo0d/gin@fd9f98e · GitHub	MISC	github.com	
Improper Input Validation in github.com/gin-gonic/gin CVE-2023-26125 Snyk	MISC	security.snyk.io	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

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](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)