



Improper Validation of Specified Quantity in Input in GitLab

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

Summary

CVE	CVE-2025-12664
State	PUBLISHED
Assigner	GitLab
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-08 23:16:56 UTC
Updated	2026-04-14 17:04:59 UTC
Description	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 13.0 before 18.8.9, 18.9 before 18.9.5, and 18.

Risk And Classification

Primary CVSS: v3.1 7.5 HIGH from cve@gitlab.com

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

EPSS: 0.000530000 probability, percentile 0.163910000 (date 2026-04-15)

Problem Types: CWE-1284 | CWE-1284 CWE-1284: Improper Validation of Specified Quantity in Input

Version	Source	Type	Score	Severity	Vector
3.1	cve@gitlab.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	CVSS	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	Gitlab	Gitlab	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	GitLab	GitLab	affected 13.0 18.8.9 semver	Not specified
CNA	GitLab	GitLab	affected 18.9 18.9.5 semver	Not specified
CNA	GitLab	GitLab	affected 18.10 18.10.3 semver	Not specified

References

Reference	Source	Link	Tags
gitlab.com/gitlab-org/gitlab/-/work_items/579376	cve@gitlab.com	gitlab.com	Broken Link
hackerone.com/reports/3377091	cve@gitlab.com	hackerone.com	Permissions Required
about.gitlab.com/releases/2026/04/08/patch-release-gitlab-18-10-3-released	cve@gitlab.com	about.gitlab.com	Vendor Advisory, Release
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: Thanks [foxribeye](https://hackerone.com/foxribeye) for reporting this vulnerability through our HackerOne bug bounty program (en)

Additional Advisory Data

Solutions

CNA: Upgrade to versions 18.8.9, 18.9.5, 18.10.3 or above.

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](#)