



# Improper Handling of Parameters in GitLab

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

## Summary

<b>CVE</b>	CVE-2026-2370
<b>State</b>	PUBLISHED
<b>Assigner</b>	GitLab
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-03-30 00:16:01 UTC
<b>Updated</b>	2026-03-30 15:44:26 UTC
<b>Description</b>	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 14.3 before 18.8.7, 18.9 before 18.9.3, and 18.

## Risk And Classification

**Primary CVSS:** v3.1 8.8 HIGH from nvd@nist.gov

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

**Problem Types:** CWE-233 | CWE-233 CWE-233: Improper Handling of Parameters

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	8.8	HIGH	<b>CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H</b>
3.1	cve@gitlab.com	Secondary	8.1	HIGH	<b>CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N</b>
3.1	CNA	CVSS	8.1	HIGH	<b>CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N</b>

## CVSS v3.1 Breakdown

Attack Vector

**Network**

Attack Complexity

**Low**

Privileges Required

**Low**

User Interaction

**None**

Scope

**Unchanged**

Confidentiality

**High**

Integrity

**High**

Availability

High

CVSS:3.1/AV:N/AC:L/PR:L/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	<a href="#">Gitlab</a>	<a href="#">Gitlab</a>	All	All	All	All
Application	<a href="#">Gitlab</a>	<a href="#">Gitlab</a>	All	All	All	All

#### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	<a href="#">GitLab</a>	<a href="#">GitLab</a>	affected 14.3 18.8.7 semver	Not specified
CNA	<a href="#">GitLab</a>	<a href="#">GitLab</a>	affected 18.9 18.9.3 semver	Not specified
CNA	<a href="#">GitLab</a>	<a href="#">GitLab</a>	affected 18.10 18.10.1 semver	Not specified

#### References

Reference	Source	Link	Tags
<a href="https://hackerone.com/reports/3522829">hackerone.com/reports/3522829</a>	<a href="mailto:cve@gitlab.com">cve@gitlab.com</a>	<a href="https://hackerone.com">hackerone.com</a>	Permissions Required
<a href="https://about.gitlab.com/releases/2026/03/25/patch-release-gitlab-18-10-1-released">about.gitlab.com/releases/2026/03/25/patch-release-gitlab-18-10-1-released</a>	<a href="mailto:cve@gitlab.com">cve@gitlab.com</a>	<a href="https://about.gitlab.com">about.gitlab.com</a>	Patch, Release Notes
<a href="https://gitlab.com/gitlab-org/gitlab/-/work_items/589635">gitlab.com/gitlab-org/gitlab/-/work_items/589635</a>	<a href="mailto:cve@gitlab.com">cve@gitlab.com</a>	<a href="https://gitlab.com">gitlab.com</a>	Broken Link
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

#### Vendor Comments And Credit

##### Discovery Credit

**CNA:** Thanks [maksyche](https://hackerone.com/maksyche) for reporting this vulnerability through our HackerOne bug bounty program (en)

#### Additional Advisory Data

##### Solutions

**CNA:** Upgrade to versions 18.8.7, 18.9.3, 18.10.1 or above.

There are currently no legacy QID mappings associated with this CVE.

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](#).

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