



# Improper Neutralization of CRLF Sequences ('CRLF Injection') in GitLab

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

## Summary

<b>CVE</b>	CVE-2026-3848
<b>State</b>	PUBLISHED
<b>Assigner</b>	GitLab
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-03-11 16:16:47 UTC
<b>Updated</b>	2026-04-16 16:38:34 UTC
<b>Description</b>	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 8.11 before 18.7.6, 18.8 before 18.8.6, and 18.9 before 18.9.6.

## Risk And Classification

**Primary CVSS:** v3.1 5 MEDIUM from cve@gitlab.com

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

**Problem Types:** CWE-93 | CWE-93 CWE-93: Improper Neutralization of CRLF Sequences ('CRLF Injection')

Version	Source	Type	Score	Severity	Vector
3.1	cve@gitlab.com	Secondary	5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:N/A:N
3.1	CNA	CVSS	5	MEDIUM	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:N/A:N

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Changed

Confidentiality

Low

Integrity

Low

None

Availability

None

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

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gitlab	Gitlab	All	All	All	All
Application	Gitlab	Gitlab	All	All	All	All

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	GitLab	GitLab	affected 8.11 18.7.6 semver	Not specified
CNA	GitLab	GitLab	affected 18.8 18.8.6 semver	Not specified
CNA	GitLab	GitLab	affected 18.9 18.9.2 semver	Not specified

### References

Reference	Source	Link	Tags
<a href="https://about.gitlab.com/releases/2026/03/11/patch-release-gitlab-18-9-2-released">about.gitlab.com/releases/2026/03/11/patch-release-gitlab-18-9-2-released</a>	cve@gitlab.com	<a href="https://about.gitlab.com">about.gitlab.com</a>	Release Notes, Vendor Ac
<a href="https://gitlab.com/gitlab-org/gitlab/-/work_items/577298">gitlab.com/gitlab-org/gitlab/-/work_items/577298</a>	cve@gitlab.com	<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 [shelld3c](https://hackerone.com/shells3c) for reporting this vulnerability. (en)

### Additional Advisory Data

Solutions

**CNA:** Upgrade to versions 18.7.6, 18.8.6, 18.9.2 or above.

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

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)