



# Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') in GitLab

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

## Summary

<b>CVE</b>	CVE-2026-6073
<b>State</b>	PUBLISHED
<b>Assigner</b>	GitLab
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-05-14 06:16:24 UTC
<b>Updated</b>	2026-05-14 06:16:24 UTC
<b>Description</b>	GitLab has remediated an issue in GitLab EE affecting all versions from 18.7 before 18.9.7, 18.10 before 18.10.6, and 18.1

## Risk And Classification

**Primary CVSS:** v3.1 8.7 HIGH from cve@gitlab.com

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

**Problem Types:** CWE-79 | CWE-79 CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Version	Source	Type	Score	Severity	Vector
3.1	cve@gitlab.com	Secondary	8.7	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:N
3.1	CNA	CVSS	8.7	HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:N

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

Required

Scope

Changed

Confidentiality

High

Integrity

High

Availability

None

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	<a href="#">GitLab</a>	<a href="#">GitLab</a>	affected 18.7 18.9.7 semver	Not specified
CNA	<a href="#">GitLab</a>	<a href="#">GitLab</a>	affected 18.10 18.10.6 semver	Not specified
CNA	<a href="#">GitLab</a>	<a href="#">GitLab</a>	affected 18.11 18.11.3 semver	Not specified

### References

Reference	Source	Link	Tags
<a href="https://gitlab.com/gitlab-org/gitlab/-/work_items/596340">gitlab.com/gitlab-org/gitlab/-/work_items/596340</a>	<a href="mailto:cve@gitlab.com">cve@gitlab.com</a>	<a href="https://gitlab.com">gitlab.com</a>	
<a href="https://hackerone.com/reports/3655677">hackerone.com/reports/3655677</a>	<a href="mailto:cve@gitlab.com">cve@gitlab.com</a>	<a href="https://hackerone.com">hackerone.com</a>	
<a href="https://about.gitlab.com/releases/2026/05/13/patch-release-gitlab-18-11-3-released">about.gitlab.com/releases/2026/05/13/patch-release-gitlab-18-11-3-released</a>	<a href="mailto:cve@gitlab.com">cve@gitlab.com</a>	<a href="https://about.gitlab.com">about.gitlab.com</a>	
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 [joaxcar](<https://hackerone.com/joaxcar>) for reporting this vulnerability through our HackerOne bug bounty program (en)

### Additional Advisory Data

#### Solutions

**CNA:** Upgrade to versions 18.9.7, 18.10.6, 18.11.3 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](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)