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

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2026-6073
State	PUBLISHED
Assigner	GitLab
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-14 06:16:24 UTC
Updated	2026-05-14 06:16:24 UTC
Description	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

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	GitLab	GitLab	affected 18.7 18.9.7 semver	Not specified
CNA	GitLab	GitLab	affected 18.10 18.10.6 semver	Not specified
CNA	GitLab	GitLab	affected 18.11 18.11.3 semver	Not specified

References

Reference	Source	Link	Tags
gitlab.com/gitlab-org/gitlab/-/work_items/596340	cve@gitlab.com	gitlab.com	
hackerone.com/reports/3655677	cve@gitlab.com	hackerone.com	
about.gitlab.com/releases/2026/05/13/patch-release-gitlab-18-11-3-released	cve@gitlab.com	about.gitlab.com	
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 [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.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**