



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

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

Summary

CVE	CVE-2026-5262
State	PUBLISHED
Assigner	GitLab
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-22 17:16:44 UTC
Updated	2026-04-22 21:23:52 UTC
Description	GitLab has remediated an issue in GitLab CE/EE affecting all versions from 16.1.0 before 18.9.6, 18.10 before 18.10.4, and

Risk And Classification

Primary CVSS: v3.1 8 HIGH from cve@gitlab.com

CVSS: 3.1/AV:N/AC:H/PR:N/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	HIGH	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:N
3.1	CNA	CVSS	8	HIGH	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:N

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

Required

Scope

Changed

Confidentiality

High

Integrity

High

Availability

None

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	GitLab	GitLab	affected 16.1.0 18.9.6 semver	Not specified
CNA	GitLab	GitLab	affected 18.10 18.10.4 semver	Not specified
CNA	GitLab	GitLab	affected 18.11 18.11.1 semver	Not specified

References

Reference	Source	Link	Tags
gitlab.com/gitlab-org/gitlab/-/work_items/595332	cve@gitlab.com	gitlab.com	
hackerone.com/reports/3574642	cve@gitlab.com	hackerone.com	
about.gitlab.com/releases/2026/04/22/patch-release-gitlab-18-11-1-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 18.9.6, 18.10.4, 18.11.1 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