CVE-2026-97229

GitLab Community Edition and Enterprise Edition Integer Overflow or Wraparound Vulnerability

Exigent | CISA KEV since Oct 29, 2026 | Actively exploited

GitLab has remediated an issue in GitLab CE/EE affecting all versions from 19.2 before 19.2.8, 19.3 before 19.3.5, and 19.4 before 19.4.2 that, under certain conditions, could have allowed an unauthenticated user to execute arbitrary code on the GitLab server via a specially crafted regular expression in a CI/CD configuration, due to insufficient regular expression validation.

EVRS	CVSS V3.1	EPSS	CISA DEADLINE
85/100	10.0	0.184	Nov 1, 2026
Immediate priority	Critical · NVD	97.2nd percentile · FIRST	CISA federal deadline in 2 days

Signals behind the score

☑ counted in the score ☐ not counted — evidence for 6 of 8 signals

☑ **CISA KEV**	Listed in the catalog	☐ **Vendor exploitation**	Confirmed exploitation in the wild
☐ **Ransomware**	No known ransomware campaign association	☑ **KEV recency**	Added to CISA KEV within the last 30 days
☑ **EPSS**	0.184 probability	☐ **Pre-patch disclosure**	Disclosure status unavailable
☑ **CVSS**	Base score 10.0	☐ **Microsoft Exploitability Index**	Not a Microsoft CVE

Remediation

Out-of-band / urgent — Patch or fixed version identified

CISA required action: Apply mitigations in accordance with vendor instructions, ensuring compliance with CISA's BOD 26-04 Prioritizing Security Updates Based on Risk (see URL in Notes) guidance and CISA's "Forensics Triage Requirements" (see URL in Notes). Follow applicable BOD 26-04 guidance for cloud services or discontinue use of the product if mitigations are unavailable. Stakeholders are responsible for evaluating each asset's internet exposure and ensuring adherence to BOD 26-04 patching guidelines. **CISA note:** Other products can potentially be affected by the same underlying Ruby/Onigmo Integer Overflow issue in CI/CD Regular Expression Compiler.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
gitlab	⩾ 19.2.0 < 19.2.8 ⩾ 19.3.0 < 19.3.5 ⩾ 19.4.0 < 19.4.2	no fixed version listed	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-9hj5-r43h-h3xg	**ruby-lang.org**	ruby-lang.org/en/news/2026/10/23/regexp-fixes-for-gitlab-cves
docs.gitlab.com	docs.gitlab.com/releases/patches/patch-release-gitlab-19-4-2-released/	**BOD 26-04**	cisa.gov/news-events/directives/bod-26-04-prioritizing-security-updates-based-risk
Forensics Triage Requirements	cisa.gov/news-events/directives/bod-26-04-implementation-guidance-prioritizing-security-updates-based-risk	**NVD**	nvd.nist.gov/vuln/detail/CVE-2026-97229
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	**ENISA EUVD**	euvd.enisa.europa.eu/vulnerability/EUVD-2026-98214
Current data	evulnable.com/vulnerability-management/cve/CVE-2026-97229		

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.