

CVE-2021-22175

GitLab Server-Side Request Forgery (SSRF) Vulnerability

CISA KEV since Feb 18, 2026

Actively exploited

When requests to the internal network for webhooks are enabled, a server-side request forgery vulnerability in GitLab affecting all versions starting from 10.5 was possible to exploit for an unauthenticated attacker even on a GitLab instance where registration is disabled

EVRS 77 / ₁₀₀ Urgent priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.534 99th percentile · FIRST	CISA DEADLINE Mar 11, 2026 CISA federal deadline · Overdue by 7 months
---	---	---	---

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 year
☒ EPSS	0.534 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
gitlab	≥ 10.5.0 < 13.6.7 ≥ 13.7.0 < 13.7.7 ≥ 13.8.0 < 13.8.4	13.6.7 · 13.7.7 · 13.8.4	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-4gm2-v7j4-74p8	Additional guidance	gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22175.json
NVD	nvd.nist.gov/vuln/detail/CVE-2021-22175	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2021-9321	Current data	evulnabile.com/vulnerability-management/cve/CVE-2021-22175

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