

CVE-2021-39935

GitLab Community and Enterprise Editions Server-Side Request Forgery (SSRF) Vulnerability

CISA KEV since Feb 3, 2026

Actively exploited

An issue has been discovered in GitLab CE/EE affecting all versions starting from 10.5 before 14.3.6, all versions starting from 14.4 before 14.4.4, all versions starting from 14.5 before 14.5.2. Unauthorized external users could perform Server Side Requests via the CI Lint API

EVRS 75_{/100} Urgent priority	CVSS V3.1 7.5 High · NVD	EPSS 0.361 98.5th percentile · FIRST	CISA DEADLINE Feb 24, 2026 CISA federal deadline · Overdue by 8 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	0.361 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.5	☐ 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	$\geq 10.5.0 < 14.3.6$ $\geq 14.4.0 < 14.4.4$ $\geq 14.5.0 < 14.5.2$	14.3.6 · 14.4.4 · 14.5.2	NVD

Sources

Vendor guidance	gitlab.com/gitlab-org/gitlab/-/issues/346187	about.gitlab.com	about.gitlab.com/releases/2021/12/06/security-release-gitlab-14-5-2-released/
NVD	nvd.nist.gov/vuln/detail/CVE-2021-39935	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2021-26291	Current data	evulnabile.com/vulnerability-management/cve/CVE-2021-39935

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