

SECURITY ADVISORY

GitLab Community Edition and Enterprise Edition exploited

CVE-2026-97229 · on CISA's exploited list since 29 October 2026

Analysis Report

CISA added CVE-2026-97229 to its exploited list on 29 October 2026; its date is 1 November 2026. What it is, who is affected, and what to do first.

PREPARED BY	NamiQ	DATE	30 October 2026
FACTS AS OF	30 October 2026	VERSION	1.0
SEVERITY	Critical: CVSS 3.1 10.0	STATUS	On CISA's exploited list; due 1 November 2026

NamiQ © 2026 NamiQ. All rights reserved. This document is the property of NamiQ. It may be shared unaltered, with attribution.

Companion article: namiq.io/insights/gitlab-community-edition-and-enterprise-cve-2026-97229

The short version

CISA added GitLab Community Edition and Enterprise Edition (CVE-2026-97229) to its list of exploited vulnerabilities on 29 October 2026. That list holds only flaws CISA has evidence are being used in attacks.

Its deadline for US federal agencies is 1 November 2026. Treat it as a date to aim for. It does not bind you.

The base score is 10 (CVSS 3.1). EPSS, the estimated chance of exploitation in the next 30 days, is 0.27. Read on 30 October 2026.

Our reading

An attacker with no account can run their own code on the GitLab server. They do it by sending a specially crafted regular expression in a CI/CD configuration. The record says this applies under certain conditions, and it does not say what they are.

Anyone running a GitLab Community or Enterprise Edition server on the 19.2, 19.3 or 19.4 release lines. Look first at any server that people without an account can reach.

What happened

GitLab Community Edition and Enterprise Edition contain a integer overflow or wraparound vulnerability that could allow 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.

That is CISA's description from its catalogue entry.

The CVE record, published by GitLab on 13 October 2026, says:

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.

Are you affected?

The record lists these versions of GitLab as affected:

- 19.2 up to, but not including, 19.2.8
- 19.3 up to, but not including, 19.3.5
- 19.4 up to, but not including, 19.4.2

The affected ranges end before 19.2.8, 19.3.5, 19.4.2. Those are the first versions the record does not list as affected. Confirm them in the vendor's advisory before you rely on them.

If you run it, find the version number first. If you cannot say what you run, that is the first job, and your IT provider can answer it in minutes.

What to do first

CISA's required action:

Apply mitigations in accordance with vendor instructions.

CISA's date is 1 November 2026. In order:

- List every GitLab server your firm or provider runs, including old test ones, and write down each version.
- Find out which of those servers can be reached by someone without an account, because the flaw needs no login.
- Treat any server on 19.2, 19.3 or 19.4 as exposed until its version is checked against the fixed releases GitLab lists.
- CISA's wording adds that you should stop using the product if no mitigation is available.
- If you cannot do it today, write down who owns it, the new date, and what limits exposure until then, such as restricting the interface to administrator networks.

How to check it is fixed

- The product reports a version outside the affected list. Read it from the product itself, not from an old inventory.
- Save the output or a screenshot with the date, so you can show later when it was done.

If it was exposed before you updated

CISA lists this because attacks have happened. An update closes the hole. It does not tell you whether someone used it first. Look in the product's logs and the web server's logs for the weeks before the update, and for accounts or files you did not create. CISA's required action also points to its forensic triage requirements (BOD 26-04).

- CI/CD configuration files that are new or recently edited, especially with odd or very long regular expressions.
- Unexpected processes, new accounts or new scheduled tasks on the GitLab server, since the flaw allows code to run there.
- Pipeline or configuration requests from users with no account.

The weakness behind it

The record classes this as CWE-190 (Integer Overflow or Wraparound).

What we could not confirm

- CISA records ransomware use as not recorded. That means not recorded, not that none has happened. No attacker is named in the sources.
- We have not tested this against any environment. This note reports what the sources say and what we would check first.
- Version ranges are as the CVE record state them. The vendor's advisory wins where it differs.
- EPSS and scores move. The figures are as at 30 October 2026.
- The paragraphs headed "Our reading" and the numbered steps are our interpretation of the sources, not a statement by CISA or the vendor.

Appendix 1. Severity decoded

CVE-2026-97229: score 10, CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H As the CVE record gives it. The record's own score can differ from the base score on the NVD record.

Metric	Value	What it means here
Attack vector	Network	Reachable over a network, with no need to be on the same segment.
Attack complexity	Low	No special conditions beyond the flaw itself.
Privileges required	None	No account is needed.
User interaction	None	No one has to do anything.
Scope	Changed	Damage reaches beyond the vulnerable component.
Confidentiality	High	Total loss of confidentiality.
Integrity	High	Total loss of integrity.
Availability	High	Total loss of availability.

Appendix 2. Timeline

Date	Event
13 October 2026	CVE record published by GitLab.
29 October 2026	CISA added it to its list of exploited vulnerabilities.
30 October 2026	The facts in this report were read.
1 November 2026	CISA's deadline for US federal agencies.

Appendix 3. Definition of done

- Every GitLab Community Edition and Enterprise Edition you run is listed, with its version.
- Each is outside the affected list, or the vendor's mitigation is in place.
- The version output or a screenshot is saved with the date.
- Logs for the weeks before the update were searched, and anything odd was written down.
- Anything not done has an owner and a date.

Sources

- CISA Known Exploited Vulnerabilities catalogue: <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>
- CVE record for CVE-2026-97229: <https://www.cve.org/CVERecord?id=CVE-2026-97229>
- FIRST: Exploit Prediction Scoring System: <https://www.first.org/epss/>
- Reference in the CVE record: gitlab.com: https://gitlab.com/gitlab-org/gitlab/-/work_items/630686
- Reference in the CVE record: hackerone.com: <https://hackerone.com/reports/4055749>
- Reference in the CVE record: hackerone.com: <https://hackerone.com/reports/4058589>
- Reference in the CVE record: docs.gitlab.com: <https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-4-2-released/>