# GitLab CVE-2026-97229 ? 60-Minute Runbook

CVSS 10.0 ? public proof-of-concept

Fixed by: GitLab 19.2.8 / 19.3.5 / 19.4.2 or newer

Maximum-severity flaw in GitLab’s CI/CD regular expression compiler: an attacker can run code on the GitLab server, no login required on instances with open sign-ups. Patch shipped October 12, 2026; a working proof-of-concept went public October 13; Censys counted 25,766 internet-facing hosts still on vulnerable versions at checker publication.

## Minutes 0-5 ? Confirm your version

1. On the GitLab host run: sudo gitlab-rake gitlab:env:info | grep "GitLab version"

2. 19.2.0-19.2.7, 19.3.0-19.3.4 or 19.4.0-19.4.1 -> EXPOSED.

3. Older than 19.2 -> no patch exists on your branch; upgrade to a supported patched release regardless.

4. 19.2.8, 19.3.5, 19.4.2 or newer -> patched; skip to the minute 50-60 block.

## Minutes 5-10 ? Check whether open sign-ups make it worse

1. Admin area -> Settings -> General -> Sign-up restrictions, or on the host: grep "signup_enabled" /etc/gitlab/gitlab.rb

2. Sign-ups open -> treat this as fully unauthenticated RCE: any internet user can plant the malicious CI config.

3. Sign-ups restricted -> an attacker still only needs one low-privilege account. Do not relax.

## Minutes 10-15 ? Snapshot before you touch anything

1. Run a GitLab backup (sudo gitlab-backup create) or take a VM snapshot, including gitlab-secrets.json, before upgrading.

## Minutes 15-35 ? Upgrade now, outside the patch cycle

1. Upgrade GitLab to 19.2.8 / 19.3.5 / 19.4.2 immediately ? outside your normal patch cycle.

2. This is the third regex-engine flaw in GitLab in a month; the component is being actively probed.

## Minutes 35-50 ? Rotate what the app worker could read

1. Rotate CI/CD variables (masked and protected first), runner registration tokens, personal access tokens, and the Rails secret in gitlab-secrets.json. Patching does not un-read secrets.

2. Turn off open registration unless you truly need it ? it is the difference between "needs an account" and "needs nothing".

## Minutes 50-60 ? Hunt and verify

1. Hunt for unauthenticated hits on the CI lint endpoint since October 12: grep "ci/lint" /var/log/gitlab/gitlab-rails/production.log

2. Review .gitlab-ci.yml commits from the last two weeks for complex regex you did not authorize, plus unexpected runner registrations or new admin users. Log review is indicative, not conclusive.

3. Re-run the version check and record versions before/after and the rotation list.

Source: Fleet checker: gitlab-cve-2026-97229.html (disclosed Oct 12, 2026; PoC Oct 13, 2026)

Generated by BreachHunter (Ingenious AI) from the fleet’s published exposure checker for this CVE. Assessment guidance only ? verify eac