Critical GitLab CE/EE flaw (CVE-2026-97229) allows unauthenticated code execution



GitLab fixed 24 security issues on 12 October 2026, including a CVSS 10.0 flaw that lets an unauthenticated attacker run code on the server. CERT-EU urges upgrading self-managed instances, internet-facing ones first.

- CVE-2026-97229 (CVSS 10.0) sits in the CI/CD regular expression compiler and permits remote code execution without authentication.
- Affected: self-managed GitLab CE/EE before 19.4.2, 19.3.4 and 19.2.8.
- Fixed releases are 19.4.2, 19.3.4 and 19.2.8, published on 12 October 2026.
- The release also fixes an XSS flaw (CVSS 8.7), an authorisation flaw on protected branches (CVSS 8.5) and a cache poisoning bug (8.2) that could expose protected CI/CD variables.
- CERT-EU advises upgrading internet-facing instances first.

GitLab has released versions 19.4.2, 19.3.4 and 19.2.8 of its Community and Enterprise Editions. The update fixes 24 security issues, one of them critical. CERT-EU published an advisory on the release on 12 October 2026.

The critical flaw

CVE-2026-97229 carries a CVSS score of 10.0. It is located in the CI/CD regular expression compiler. Weak validation of regular expressions leads to an integer overflow, and a specially crafted expression in a CI/CD configuration can then trigger code execution. An unauthenticated attacker could use it to run arbitrary code on the server.

Other fixes in the same release

- CVE-2026-92883 (CVSS 8.7): cross-site scripting in syntax highlighting, allowing an authenticated user to run JavaScript in other users' browsers through a crafted repository.
- CVE-2026-16301 (CVSS 8.5): an authorisation flaw that lets a developer run pipelines on protected branches without permission.
- 21 further issues, including a cache poisoning bug rated 8.2 that could expose protected CI/CD variables.

What to do

The flaws affect self-managed GitLab CE/EE instances running versions before 19.4.2, 19.3.4 or 19.2.8. CERT-EU strongly recommends upgrading all such instances to a fixed version as soon as possible, beginning with those reachable from the internet. Institutions should identify where GitLab is hosted, confirm the running version and schedule the upgrade without delay.

What to do now

1. Inventory all self-managed GitLab CE/EE instances and record their versions.
2. Upgrade to 19.4.2, 19.3.4 or 19.2.8 (matching your release line), starting with internet-facing instances.
3. Where upgrade must wait, restrict network access to the instance to trusted ranges.
4. After patching, review CI/CD configurations and pipeline run history for unexpected changes or activity.
5. Consider rotating protected CI/CD variables if exposure is suspected, given the cache poisoning issue.
6. Record the change under your vulnerability and patch management process.