Attempted Exploit of CVSS 10.0 GitLab Flaw Hit Alpine Linux's Own Server



Alpine Linux reported an attempt to exploit CVE-2026-97229 (CVSS 10.0) on its GitLab server, a week after GitLab issued a fix. Alpine found no evidence the attack worked.

- Alpine Linux said on 28 October that an attacker tried to exploit a critical GitLab flaw on its own GitLab server.
- The flaw is CVE-2026-97229, with a CVSS score of 10.0.
- It can allow code execution on a GitLab server through a crafted regular expression in a CI configuration.
- The attempt came a week after GitLab released a fix.
- Alpine found no evidence that the attack succeeded.

What happened

Alpine Linux said on 28 October that an attacker tried to exploit a critical GitLab vulnerability on the project's own GitLab server. The attempt took place a week after GitLab had released a fix for the flaw.

The vulnerability is tracked as CVE-2026-97229 and carries a CVSS score of 10.0. According to the report, it can let an attacker run code on a GitLab server by using a crafted regular expression in a CI configuration. Alpine found no evidence that the attack worked.

Why it matters

The case shows that attempts against a critical flaw can begin within days of a fix being published. Organisations that host their own GitLab instances, particularly those whose CI pipelines build or deploy internal software, should treat the gap between a patch release and its installation as a period of real exposure.

The source does not provide further technical detail, such as affected versions or the fixed release numbers, so those should be taken from GitLab's own advisory.

What to do next

Confirm whether your organisation runs self-managed GitLab, check the vendor advisory for CVE-2026-97229, and apply the fix without waiting for the next routine patch cycle. Then review logs for unusual CI configuration changes or unexpected activity around the time of the fix release.

What to do now

1. Inventory all self-managed GitLab instances, including those used by development and DevOps teams.
2. Check GitLab's advisory for CVE-2026-97229 and apply the fix on an emergency basis.
3. Review GitLab and server logs for unusual CI configuration changes or unexpected activity.
4. Restrict network exposure of GitLab servers to what is strictly necessary.
5. Include critical-patch timelines for development tooling in your vulnerability management procedure.