GitLab patches maximum-severity code execution flaw CVE-2026-110264



GitLab has patched CVE-2026-110264, a maximum-severity integer overflow in its Regular Expression Compiler that could let unauthenticated attackers run code on self-managed servers. Upgrade CE and EE instances promptly.

- CVE-2026-110264 is an integer overflow in GitLab's Regular Expression Compiler that can allow unauthenticated remote code execution.
- Fixes are in GitLab CE and EE versions 19.5.1, 19.4.3, 19.3.6, 19.2.9, 19.1.9, 19.0.10 and 18.11.13.
- GitLab.com is already patched; GitLab Dedicated tenants on 19.3.5-internal0, 19.4.2-internal0 or later need no action.
- Shadowserver tracks over 2,700 internet-exposed GitLab CE instances, with no indication of how many are patched or honeypots.

> - This follows another critical flaw, CVE-2026-97229, disclosed ten days earlier and reported by the same researcher.

GitLab has released security updates for CVE-2026-110264, a maximum-severity flaw that can let a remote, unauthenticated attacker execute arbitrary code on a vulnerable server. The issue was reported by a researcher using the handle 'joaxcar' through GitLab's HackerOne bug bounty program.

What the flaw is

The weakness is an integer overflow in the Regular Expression Compiler, the background engine that parses and validates regular expressions in configuration files. Under certain conditions, a specially crafted expression could trigger the overflow and lead to code execution on the GitLab server.

GitLab has fixed the issue in Community Edition and Enterprise Edition versions 19.5.1, 19.4.3, 19.3.6, 19.2.9, 19.1.9, 19.0.10 and 18.11.13, and urges affected installations to upgrade as soon as possible. GitLab.com already runs the patched version. GitLab Dedicated tenants on 19.3.5-internal0 and 19.4.2-internal0 or later already include the fixes.

Wider context

Shadowserver currently tracks more than 2,700 GitLab Community Edition instances exposed online, though it does not say how many are honeypots or already secured. The source does not report exploitation of this specific flaw.

The disclosure follows CVE-2026-97229, another critical remote code execution flaw in the CI/CD Regular Expression Compiler, reported ten days earlier by the same researcher. Last month GitLab also fixed CVE-2026-85706, which let unauthenticated attackers read sensitive data; CISA added it to its list of actively exploited flaws a day later. Since November 2021, CISA has flagged five GitLab flaws exploited in the wild.

For organisations running self-managed GitLab, the practical priority is to confirm versions and apply the fixed release without delay.

What to do now

1. Inventory all self-managed GitLab CE and EE instances and confirm their versions against the fixed releases.
2. Upgrade affected instances to the patched version for your branch as a priority, ahead of routine change windows where policy allows.
3. Check whether any GitLab instance is reachable from the internet and restrict access to trusted networks or VPN where possible.
4. Review server and CI/CD logs for unusual activity, and rotate credentials and secrets stored in GitLab if

compromise is suspected.

5. Record the patching decision and timeline under your vulnerability and patch management process (NCA ECC, SAMA CSF).