

SECURITY ADVISORY

Critical GitLab CE and EE Remote Code Execution

An unauthenticated server vulnerability puts self-managed source code and delivery platforms at risk.

SEVERITY	PUBLISHED	CATEGORY	STATUS
CRITICAL	21 OCT 2026	DEVSECOPS / RCE	PATCH AVAILABLE

Reviewed 23 Oct 2026. Severity and scope details appear below.

Severity: CRITICAL · Category: DevSecOps / RCE · Status: Patch available. CVE-2026-110264 is rated CVSS v3.1 10.0. Published 21 October 2026; reviewed 23 October 2026.

URGENT ACTION

Upgrade affected self-managed GitLab CE/EE installations promptly, prioritizing internet-facing servers. Preserve evidence if compromise is suspected. Published detection rules support investigation; their availability does not itself establish active exploitation. [1, 2]

01 INCIDENT SUMMARY

GitLab released security updates on 21 October 2026 for an integer overflow in its regular expression compiler. Under certain conditions, CVE-2026-110264 allows code execution on the GitLab server without a prior login. CERT-EU and CERT-In subsequently issued critical advisories. [1-3]

The same release addresses other authorization, information-disclosure and authentication issues. This advisory prioritizes the critical RCE; apply the complete supported patch release rather than treating it as a single-issue fix. [1, 3]

02 POTENTIAL IMPACT

- Server control: Successful exploitation may allow an attacker to run code within the GitLab server environment. [1, 2]
- Development workflow exposure: Assess source repositories, accessible tokens, CI/CD secrets and connected deployment systems when investigating a suspected server compromise. This is a response priority, not a claim that every asset is automatically exposed.
- Wider access risks: The accompanying fixes also address account access, sensitive data and security-control weaknesses. [3]

03 PRIORITY ACTIONS FOR CUSTOMERS

1. Identify every self-managed instance

Record the deployed edition, version, owner, exposure and hosting model. Include secondary and recovery instances. Ask providers to confirm patch status where they operate the service.

2. Upgrade through a supported path

Select the applicable fixed release below, review upgrade prerequisites and retain a tested recovery plan. Validate the version actually running after the change. [1]

3. Investigate suspicious activity

Use GitLab's native-worker-crash and Org-mode-render-error detection guidance alongside web, application and endpoint logs. Investigate unexpected access, processes and configuration changes. A detection match needs assessment; absence of a match is not proof of safety. [1, 2]

4. Respond to confirmed compromise

Isolate affected systems, retain evidence and assess repository and deployment access. Rotate exposed credentials and restore trusted operation under the incident-response plan. Patching alone does not remove an attacker's existing access.

TECHNICAL & RESPONSE DETAILS

Guidance for infrastructure, development, operations and security teams

04 TECHNICAL INFORMATION

- Identifier / weakness: CVE-2026-110264; integer overflow in regular expression compilation. [1]
- Severity / access: Critical, CVSS v3.1 10.0; unauthenticated code execution under affected conditions. [1, 2]
- Scope: GitLab Community Edition and Enterprise Edition. GitLab.com is patched; GitLab identifies patched Dedicated tenant builds in its release notice. [1]
- Exploitation status: The reviewed sources provide detection guidance but do not establish confirmed active exploitation as of 23 October 2026. [1, 2]

05 PATCHED VERSIONS AND EXPOSURE

- Versions from 7.0 before 18.11.13: the fixed backport is 18.11.13; follow the supported upgrade path for older installations.
- 19.0, 19.1 and 19.2: fixed in 19.0.10, 19.1.9 and 19.2.9 respectively.
- 19.3, 19.4 and 19.5: fixed in 19.3.6, 19.4.3 and 19.5.1 respectively. Use the applicable fixed or newer supported release. [1-3]

06 VALIDATION CHECKLIST

- Confirm every in-scope server is running the intended fixed build.
- Test authentication, repository access, merge requests, webhooks and critical CI/CD jobs.
- Record investigation results and preserve relevant logs separately from the server.
- Track remediation owners, exceptions, provider confirmations and any exposed secrets.

ADVISORY BASIS

Independent 443 Labs customer awareness guidance. Publication date follows GitLab's 21 October release; sources were reviewed on 23 October 2026. This advisory does not establish compromise of any recipient environment.

PRIMARY SOURCES

[1] [GitLab critical patch release - 21 October 2026](#)

[2] [CERT-EU advisory 2026-019 - 22 October 2026](#)

[3] [CERT-In CIVN-2026-0516 - 22 October 2026](#)