



Security Advisory 2026-019

Critical Vulnerability in GitLab Community and Enterprise Editions

2026-10-22 — v1.0

TLP:CLEAR

History:

- 22/10/2026 — v1.0 – Initial publication

Summary

On 21 October 2026, GitLab published a security advisory addressing several vulnerabilities among which a critical flaw that could allow an unauthenticated user to execute arbitrary code on a GitLab server [1].

CERT-EU recommends organisations to update affected assets as soon as possible, prioritising internet facing assets, and to run an assessment to identify compromised assets.

Technical Details

The vulnerability **CVE-2026-110264**, with a CVSS score of 10, is a critical integer overflow vulnerability within the regular expression compiler which could allow an unauthenticated user to execute arbitrary code on the affected GitLab server.

GitLab also fixed 2 high severity, 5 medium severity and 4 low severity vulnerabilities [1].

Affected Products

The vulnerability **CVE-2026-110264** affects the following versions of GitLab Community and Enterprise Editions [1]:

- from 7.0 before 18.11.13
- 19.0 before 19.0.10
- 19.1 before 19.1.9
- 19.2 before 19.2.9
- 19.3 before 19.3.6
- 19.4 before 19.4.3
- 19.5 before 19.5.1

Recommendations

CERT-EU recommends organisations to update affected assets as soon as possible, prioritising internet facing assets, and to run an assessment to identify compromised assets.

Compromise assessment

GitLab has published two detection rules to identify exploitation attempts [1, 2, 3].

References

- [1] <https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-5-1-released/>
- [2] https://gitlab.com/gitlab-security-oss/tldr/-/blob/main/Detections/platforms/GitLab/Vulnerability%20Detections/onigmo_native_worker_crash.md?ref_type=heads
- [3] https://gitlab.com/gitlab-security-oss/tldr/-/blob/main/Detections/platforms/GitLab/Vulnerability%20Detections/org_mode_render_error_burst.md?ref_type=heads