



Security Advisory 2026-016

Critical Vulnerability in GitLab CE and EE

2026-10-12 — v1.0

TLP:CLEAR

History:

- 12/10/2026 — v1.0 – Initial publication

Summary

On 12 October 2026, GitLab released versions 19.4.2, 19.3.4 and 19.2.8 of GitLab Community Edition (CE) and Enterprise Edition (EE), fixing 24 security issues among which a **critical vulnerability** that could allow an **unauthenticated attacker** to **execute arbitrary code** on the server [1].

CERT-EU strongly recommends upgrading self-managed GitLab CE/EE instances to a fixed version as soon as possible, starting with internet-facing instances.

Technical Details

The vulnerability **CVE-2026-97229**, with a CVSS score of 10.0, is located in the CI/CD regular expression compiler [1]. 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** [1].

The same release also fixes other vulnerabilities [1]:

- **CVE-2026-92883** (CVSS: 8.7): a **cross-site scripting** flaw in syntax highlighting that lets an **authenticated user run arbitrary JavaScript in other users' browsers** through a crafted repository [1].
- **CVE-2026-16301** (CVSS: 8.5): an **authorisation flaw** that lets a **developer run pipelines on protected branches without permission** [1].
- 21 further issues, including a cache poisoning bug rated 8.2 that could expose protected CI/CD variables [1].

Affected Products

The vulnerabilities affect the following versions of self-managed **GitLab CE/EE** instances [1]:

- before 19.4.2
- before 19.3.4
- before 19.2.8

Recommendations

CERT-EU strongly recommends upgrading all self-managed GitLab CE/EE instances to a fixed version, starting with internet-facing instances [1].

References

[1] <https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-4-2-released/>