



An Láirionad Náisiúnta
Cibearshlándála
National Cyber
Security Centre

NCSC #2610230250

NCSC Advisory

Critical Vulnerability in GitLab Community
Edition (CE) and Enterprise Edition (EE)

CVE-2026-110264

23rd, October 2026

STATUS: TLP:CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

For more information on the Traffic Light Protocol, see <https://www.first.org/tlp/>.
Please treat this document in accordance with the TLP assigned.



Description

CVE ID: CVE-2026-110264

Published: 2026-10-22

Vendor: GitLab

Product: GitLab

CVSS Score¹: 10

Products Affected

Product	Version
GitLab	7.0 < 18.11.13
GitLab	19.0 < 19.0.10
GitLab	19.1 < 19.1.9
GitLab	19.2 < 19.2.9
GitLab	19.3 < 19.3.6
GitLab	19.4 < 19.4.3
GitLab	19.5 < 19.5.1

Impact

An issue has been discovered in GitLab CE/EE affecting all versions 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, and 19.5 before 19.5.1 that, under certain conditions, could have allowed an unauthenticated user to execute arbitrary code on the GitLab server due to integer overflow when compiling a specially crafted regular expression.

Common Weakness Enumeration (CWE)²: CWE-190: Integer Overflow or Wraparound

Known Exploited Vulnerability (KEV) catalog³: No

Used by Ransomware Operators: N/A

¹ <https://www.first.org/cvss/>

² <https://cwe.mitre.org>

³ <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>



Recommendations

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from GitLab.

- <https://nvd.nist.gov/vuln/detail/CVE-2026-110264>
- <https://www.cve.org/CVERecord?id=CVE-2026-110264>
- <https://hackerone.com/reports/4093475>
- <https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-5-1-released/>

