

Alert Bulletin

Bulletin N.: 118

Publication Date: 21/10/2026

Subject: Alert 2026-118 Critical vulnerability in GitLab allows unauthenticated RCE

Traffic Light Protocol (TLP): White

Affected product(s):

The vulnerability affects both GitLab CE and GitLab EE. GitLab published fixes in seven branches, including four prior to its usual maintenance window.

Product	Affected versions	Fixed version
GitLab CE / EE	From 7.0 through versions prior to 18.11.13	18.11.13
GitLab CE / EE	19.0.x prior to 19.0.10	19.0.10
GitLab CE / EE	19.1.x prior to 19.1.9	19.1.9
GitLab CE / EE	19.2.x prior to 19.2.9	19.2.9
GitLab CE / EE	19.3.x prior to 19.3.6	19.3.6
GitLab CE / EE	19.4.x prior to 19.4.3	19.4.3
GitLab CE / EE	19.5.x prior to 19.5.1	19.5.1

Description

A maximum severity vulnerability has been published (CVSSv3.1 10 – CRITICAL) in GitLab, which under certain conditions allows an unauthenticated attacker to execute arbitrary code on the server. It has been labeled as CVE-2026-110264.

The flaw affects GitLab Community Edition —CE— and Enterprise Edition —EE— since version 7.0 and originates in an integer overflow during the compilation of specially crafted regular expressions. Organizations with self-managed installations must update immediately, even if they applied the patches published on October 12, since these do not fix this new vulnerability.

The issue affects the regular expression compiler used by GitLab. A specially designed expression can trigger an integer overflow and, under certain conditions, allow code execution on the server without credentials or user interaction.

GitLab has not disclosed all the conditions necessary to reach the vulnerable component. Therefore, it is not possible to rule out exposure based solely on the instance configuration. The advisory does not offer a temporary mitigation that replaces the update.

Solution

The solution consists of updating each affected instance to one of the fixed versions of its branch or to a later version that includes the fix, following the upgrade path supported by GitLab. Priority should be given to instances exposed to the Internet, without excluding internal servers. The October 12 patches for CVE-2026-97229 do not fix CVE-2026-110264; installations updated on that date should be reviewed again.

For info on how to update, visit the following link:

<https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-5-1-released>

Additional information:

- GitLab — official advisory and fixed versions:
<https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-5-1-released/>
- The Hacker News — vulnerability analysis and scope:
<https://thehackernews.com/2026/10/critical-gitlab-flaw-cvss-100-could.html>