GitLab Releases Fix for Maximum-Severity Unauthenticated RCE Flaw in Self-Managed Servers



GitLab issued fixes on October 21 for a CVSS 10.0 flaw that lets an unauthenticated attacker run code on self-managed servers. It affects all versions back to 7.0, and administrators who patched on October 12 must update again.

- The flaw is rated CVSS 10.0 and allows code execution on a self-managed GitLab server without logging in.
- It affects every version going back to 7.0, released in 2014.
- GitLab published fixes on October 21.
- The October 12 update covered only versions 19.2 and later.
- The new fixed versions are one patch above the October 12 release, so earlier patching is not enough.

GitLab has released fixes for a critical flaw rated CVSS 10.0, the maximum score. The weakness allows an attacker to run code on a self-managed GitLab server without authenticating. According to the report, it affects every version of the software going back to 7.0, which was released in 2014.

Why earlier patching may not be enough

The fixes were published on October 21. Administrators who applied the October 12 update should not assume they are covered. That update addressed only versions 19.2 and later, and the newly fixed versions sit one patch above it. Teams that updated nine days earlier therefore still need to move to the new release.

Who is exposed

The issue concerns self-managed installations, where the organisation itself is responsible for applying updates. Because the affected range spans more than a decade of releases, older and rarely maintained instances are in scope as well as current ones. The source excerpt does not provide a CVE identifier, evidence of exploitation or workarounds, so teams should consult GitLab's own release notes for those details.

Source code repositories and CI/CD pipelines often hold credentials, deployment keys and proprietary code. An unauthenticated code-execution flaw on such a server is a serious concern for any regulated institution, and it warrants prompt, prioritised handling.

What to do now

1. Inventory all self-managed GitLab instances, including old or unmaintained ones, and record their versions.
2. Upgrade each instance to the fixed version released on October 21, even if the October 12 update was already applied.
3. Confirm the installed version after upgrading rather than relying on the change ticket alone.
4. Restrict network access to GitLab servers to trusted ranges until patching is verified.
5. Review server and pipeline logs for unusual activity and rotate credentials and deployment keys stored in GitLab if compromise is suspected.
6. Record the emergency patching in your vulnerability management and change records for audit evidence.