Security Advisory 2023-031

GitLab – Critical Path Traversal Vulnerability

May 25, 2023 — v1.0

TLP:CLEAR

History:

- *25/05/2023 — v1.0 – Initial publication*

Summary

On May 23, 2023, GitLab released an emergency security update to urgently address a critical severity path traversal flaw – **CVE-2023-2825** – with a CVSS v3.1 score of **10.0**. This issue was discovered in GitLab Community Edition (CE) and Enterprise Edition (EE) version 16.0.0, with older versions not being affected. The flaw allows an unauthenticated attacker to read arbitrary files on the server when an attachment exists in a public project nested within at least five groups [1,2].

Technical Details

The critical path traversal flaw was discovered by a security researcher known as *pwnie*. The flaw arises from a problem in the way GitLab manages or resolves paths for attached files nested within several levels of group hierarchy. It can be exploited by an unauthenticated attacker to read arbitrary files on the server, thereby potentially exposing sensitive data, including proprietary software code, user credentials, tokens, files, and other private information.

The vulnerability can only be triggered under specific conditions, i.e., when there's an attachment in a public project nested within at least five groups [1,2].

Products Affected

The issue affects GitLab Community Edition (CE) and Enterprise Edition (EE) version 16.0.0.

The older versions are not affected by this vulnerability.

Recommendations

CERT-EU strongly recommends that all installations running GitLab CE/EE version 16.0.0 be upgraded to version 16.0.1.

References

[1] https://about.gitlab.com/releases/2023/05/23/critical-security-release-gitlab-16-0-1-released/

[2] https://www.bleepingcomputer.com/news/security/gitlab-strongly-recommends-patching-max-severity-flaw-asap/