Security Advisory 2023-067

Critical Flaw in GitLab

September 20, 2023 — v1.0

TLP:CLEAR

History:

- *20/09/2023 — v1.0 – Initial publication*

Summary

On September 18, GitLab has released security updates to address a critical flaw identified by `CVE-2023-4998` that, if exploited, would allow an attacker to run code, modify data or trigger specific events within the GitLab system [1]. This could result in loss of intellectual property, damaging data leaks, supply chain attacks, and other high-risk scenarios [2].

It is strongly recommended updating as soon as possible to a fixed version.

Technical Details

The vulnerability `CVE-2023-4998` has a CVSS score of 9.6 out of 10, and is a bypass of the fix for the medium severity flaw identified as `CVE-2023-3932` [3]. By using scheduled security scan policies, it is possible for an authenticated attacker to run pipelines as an arbitrary user. Pipeline tasks are series of automated tasks that could give access to sensitive information, allow users to run code, modify data or trigger specific events.

Affected Products

The flaw impacts GitLab Community Edition (CE) and Enterprise Edition (EE) versions 13.12 through 16.2.7 and versions 16.3 through 16.3.4.

Instances running versions earlier than 16.2 are vulnerable if both *Direct transfers* [4] and *Security policies* [5] features are enabled at the same time.

Recommendations

CERT-EU strongly recommends that all installations running a version affected by the issues described above are upgraded to the latest version as soon as possible.

Workaround

For instances running versions earlier than 16.2, in order to mitigate this vulnerability in situations where it is not possible to upgrade, it is required to disable the *Direct transfers* feature and/or the *Security policies* feature.

References

[1] https://about.gitlab.com/releases/2023/09/18/security-release-gitlab-16-3-4-released/

[2] https://www.bleepingcomputer.com/news/security/gitlab-urges-users-to-install-security-updates-for-critical-pipeline-flaw/

[3] https://nvd.nist.gov/vuln/detail/CVE-2023-3932

[4] https://docs.gitlab.com/ee/administration/settings/import_and_export_settings.html#enable-migration-of-groups-and-projects-by-direct-transfer

[5] https://docs.gitlab.com/ee/user/application_security/policies/scan-execution-policies.html