Security Advisory 2024-007

Critical Vulnerabilities in GitLab

January 12, 2024 — v1.0

TLP:CLEAR

History:

- *12/01/2024 — v1.0 – Initial publication*

Summary

On January 11, 2024, GitLab released a security advisory addressing several vulnerabilities, including critical ones that, if exploited, could lead to account takeover, or slack command execution.

It is recommended upgrading as soon as possible.

Technical Details

- The vulnerability `CVE-2023-7028`, with a CVSS score of 10, allows user account password reset emails to be sent to unverified email addresses, leading to potential account takeovers.
- The vulnerability `CVE-2023-5356`, with a CVSS score of 9.6, allows a user to abuse Slack and Mattermost integrations to execute slash commands as another user.
- The vulnerability `CVE-2023-4812`, with a CVSS score of 7.6, would allow a user to bypass the required `CODEOWNERS` approval by adding changes to a previously approved merge request.

Affected Products

- The vulnerability `CVE-2023-7028` affects GitLab Community Edition (CE) and Enterprise Edition (EE) versions:
  - 16.1 prior to 16.1.6;
  - 16.2 prior to 16.2.9;
  - 16.3 prior to 16.3.7;
  - 16.4 prior to 16.4.5;
  - 16.5 prior to 16.5.6;
  - 16.6 prior to 16.6.4;
  - 16.7 prior to 16.7.2.

Within these versions, all authentication mechanisms are impacted. Additionally, users who have two-factor authentication enabled are vulnerable to password reset but not account takeover as their second authentication factor is required to login.

- The vulnerability `CVE-2023-5356` affects GitLab Community Edition (CE) and Enterprise Edition (EE) versions:
  - from 8.13 prior to 16.5.6;
  - from 16.6 prior to 16.6.4;
  - from 16.7 prior to 16.7.2.
- The vulnerability `CVE-2023-4812` affects GitLab Community Edition (CE) and Enterprise Edition (EE) versions:
  - from 15.3 prior to 16.5.5;
  - from 16.6 prior to 16.6.4;
  - from 16.7 prior to 16.7.2.

Recommendations

It is strongly recommended to upgrade all GitLab installations to one of the new versions immediately. The release also emphasises the importance of enabling Two-Factor Authentication (2FA) for additional security.

Detection

At the moment, the editor did not detect any abuse of the vulnerability `CVE-2023-7028` on platforms managed by GitLab, including `GitLab.com` and GitLab Dedicated instances. Nevertheless, regarding the self-managed instances, customers can review their logs to check for possible attempts to exploit this vulnerability:

- Check *"gitlab-rails/production_json.log"* for HTTP requests to the `/users/password` path with `params.value.email` consisting of a JSON array with multiple email addresses.
- Check *"gitlab-rails/audit_json.log"* for entries with `meta.caller.id` of `PasswordsController#create` and `target_details` consisting of a JSON array with multiple email addresses.

References

[1] https://about.gitlab.com/releases/2024/01/11/critical-security-release-gitlab-16-7-2-released/