Security Advisory 2022-004

Multiple Vulnerabilities in GitLab

January 17, 2022 — v1.0

TLP:WHITE

History:

- *17/01/2022 — v1.0 – Initial publication*

Summary

On January 11th, GitLab released significant security updates to address multiple vulnerabilities, including an arbitrary file read issue rated as 'critical' and two high-impact vulnerabilities, among others. The update tackles a vulnerability involving cross-site scripting (XSS) in Notes, along with a high-impact authentication-related flaw involving a lack of state parameter on GitHub import project OAuth.

Gitlab strongly encourages users to upgrade to 14.6.2, 14.5.3, or 14.4.5 for GitLab Community Edition (CE) and Enterprise Edition (EE), in order to safeguard their environments [1].

Technical Details

Critical Vulnerability

- Arbitrary file read via group import feature (CVE ID has not been assigned yet).

An issue has been discovered in GitLab CE/EE affecting all versions starting with 14.5. Arbitrary file read was possible by importing a group due to incorrect file handling [2].

High Severity Vulnerabilities

- **CVE-2021-39946**

Stored Cross-Site Scripting (XSS) in Notes. Improper neutralisation of user input in GitLab CE/EE versions 14.3 to 14.3.6, 14.4 to 14.4.4, and 14.5 to 14.5.2 allowed an attacker to exploit XSS by abusing the generation of the HTML code related to emojis [2].

- **CVE-2022-0154**

Lack of state parameter on GitHub import project OAuth. An issue has been discovered in GitLab affecting all versions starting from 7.7 before 14.4.5, all versions starting from 14.5.0 before 14.5.3, and all versions starting from 14.6.0 before 14.6.2. GitLab was vulnerable to a Cross-Site Request Forgery attack that allows a malicious user to have their GitHub project imported on another GitLab user account [2].

Other Vulnerabilities

Additionally to the critical and high severity vulnerabilities mentioned above, Gitlab announced several others, most notably:

- CVE-2022-0152
- CVE-2022-0151
- CVE-2022-0172
- CVE-2022-0090
- CVE-2022-0125
- CVE-2022-0124
- CVE-2021-39942
- CVE-2022-0093
- CVE-2021-39927

Affected Products

- GitLab Community Edition (CE) versions prior to 14.6.2, 14.5.3, and 14.4.5
- GitLab Enterprise Edition (EE) versions prior to 14.6.2, 14.5.3, and 14.4.5

Recommendations

CERT-EU recommends updating to the latest versions of GitLab Community Edition (CE) and Enterprise Edition (EE) **as soon as possible** [3, 4].

References

[1] https://portswigger.net/daily-swig/gitlab-shifts-left-to-patch-high-impact-vulnerabilities

[2] https://about.gitlab.com/releases/2022/01/11/security-release-gitlab-14-6-2-released/

[3] https://about.gitlab.com/update/

[4] https://docs.gitlab.com/runner/install/linux-repository.html#updating-the-runner