CERT-EU

Security Advisory 2024-051

Vulnerabilities in GitLab

May 22, 2024 — v1.0

TLP:CLEAR

History:

- *27/05/2024 — v1.0 – Initial publication*

Summary

On May 22, GitLab has released several versions for GitLab Community Edition (CE) and Enterprise Edition (EE) containing important bug and security fixes [1]. These fixes notably address a vulnerability that would allow an attacker to take accounts over via an XSS vulnerability.

It is strongly recommended upgrading affected versions to the latest version as soon as possible.

Technical Details

The vulnerability **CVE-2024-4835**, with a CVSS score of 8.0, is due to an XSS weakness within GitLab. By leveraging this condition via the VS code editor (Web IDE), an attacker can craft a malicious page to exfiltrate sensitive user information. User interaction is needed to exploit this vulnerability, increasing the attacks' complexity.

Affected Products

All GitLab Community Edition (CE) and Enterprise Edition (EE) versions up to 16.10.6, versions 16.11 up to 16.11.3, and 17.0 up to 17.0.1 are affected by at least one of the vulnerabilities [1].

Recommendations

It is strongly recommended upgrading affected versions to the latest version as soon as possible.

References

[1] https://about.gitlab.com/releases/2024/05/22/patch-release-gitlab-17-0-1-released/