10 years CERT-EU

Security Advisory 2025-020

High Severity Vulnerabilities in Gitlab Products

2025-06-12 — v1.0

TLP:CLEAR

History:

- *12/06/2025 — v1.0 – Initial publication*

Summary

On 11 June 2025, Gitlab released security updates for their products addressing multiple vulnerabilities in Gitlab Community Edition (CE) and Enterprise Edition (EE) [1].

It is recommended updating affected Gitlab installations as soon as possible.

Technical Details

The vulnerability **CVE-2025-4278**, with a CVSS score of 8.7, is an issue that, under certain conditions, could have allowed a successful attacker to achieve account takeover by injecting code into the search page.

The vulnerability **CVE-2025-2254**, with a CVSS score of 8.7, is a cross-site scripting (XSS) issue that, under certain conditions, could have allowed a successful attacker to act in the context of a legitimate user by injecting a malicious script into the snippet viewer.

The vulnerability **CVE-2025-5121**, with a CVSS score of 8.5, is a missing authorisation vulnerability that, under certain conditions, could have allowed a successful attacker with authenticated access to a GitLab instance with a GitLab Ultimate license applied (paid customer or trial) to inject a malicious CI/CD job into all future CI/CD pipelines of any project.

The vulnerability **CVE-2025-0673**, with a CVSS score of 7.5, is an issue that could have allowed a successful attacker to deny access to legitimate users of the targeted system by triggering an infinite redirect loop causing memory exhaustion on the server.

Gitlab also fixes 5 medium and 1 low severity vulnerabilities.

Affected Products

The following products and versions are affected by one or more high severity vulnerabilities [1]:

- GitLab CE/EE: all versions from 7.7 before 17.10.8, 17.9 before 17.10.8, 17.11 before 17.11.4, and 18.0 before 18.0.2
- GitLab Ultimate EE from 17.11 before 17.11.4 and 18.0 before 18.0.2

Recommendations

It is recommended updating affected Gitlab installations as soon as possible.

References

[1] https://about.gitlab.com/releases/2025/06/11/patch-release-gitlab-18-0-2-released/