مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates- GitLab

Tracking #:432319116

Date:12-06-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed GitLab has released security updates addressing multiple vulnerabilities affecting GitLab Community Edition (CE) and Enterprise Edition (EE).

TECHNICAL DETAILS:

GitLab has released security updates addressing multiple vulnerabilities affecting GitLab Community Edition (CE) and Enterprise Edition (EE). The vulnerabilities range from Critical business-impacting access control issues to Denial of Service (DoS), Cross-Site Scripting (XSS), Server-Side Request Forgery (SSRF), Authorization Bypass, and HTML Injection flaws.

The most severe vulnerability, CVE-2026-6552 (CVSS 8.7), could allow a Group Owner to take over another group member's GitLab account through improper authorization in the Group SAML Identity API. Another significant vulnerability, CVE-2026-10087 (CVSS 8.7), enables authenticated attackers to execute arbitrary client-side code via stored XSS in the Analytics Dashboard.

Vulnerability Details:

1. CVE-2026-6552 — High (CVSS 8.7) — Improper Access Control in Group SAML Identity API allowing a Group Owner to potentially take over another group member's GitLab account.
2. CVE-2026-10087 — High (CVSS 8.7) — Stored Cross-Site Scripting (XSS) in Analytics Dashboard enabling authenticated users to execute arbitrary client-side code in a victim's browser.
3. CVE-2026-7250 — High (CVSS 7.5) — Denial of Service vulnerability in Grape API JSON parsing middleware allowing unauthenticated attackers to disrupt GitLab services.
4. CVE-2026-8589 — High (CVSS 7.3) — HTML Injection in group settings fields that could enable unauthorized email address addition to user accounts.
5. CVE-2026-1500 — Medium (CVSS 6.5) — Denial of Service vulnerability in Group Placeholder Reassignments API through specially crafted file uploads causing resource exhaustion.
6. CVE-2026-6269 — Medium (CVSS 5.4) — Improper Access Control in Merge Requests API allowing developers to modify hidden merge requests.
7. CVE-2026-9204 — Medium (CVSS 5.3) — Server-Side Request Forgery (SSRF) in Gitaly repository import potentially allowing access to internal network resources and arbitrary file reads.
8. CVE-2026-10733 — Medium (CVSS 4.3) — HTML Injection in CI/CD Catalog that may lead to denial of service conditions affecting catalog availability.
9. CVE-2026-6277 — Medium (CVSS 4.3) — Improper Access Control in Security Inventory allowing unauthorized management of project security configurations.
10. CVE-2026-6976 — Low (CVSS 3.7) — Authorization Bypass in Merge Request diff views allowing changes to be hidden from reviewers.
11. CVE-2026-3553 — Low (CVSS 3.1) — Improper Access Control in Todos API exposing confidential issue information to unauthorized users.
12. CVE-2026-9694 — Low (CVSS 2.6) — Improper Neutralization in Service Desk email templates enabling content injection and Support Bot impersonation.

Note: Refer to the Gitlab advisory for release notes and additional information.

Fixed Versions:

- 19.0.2
- 18.11.5
- 18.10.8

RECOMMENDATIONS:

Immediate Actions:

- Organizations running affected GitLab versions should prioritize upgrading to fixed version.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-0-2-released/#cve-2026-6552---improper-access-control-issue-in-group-saml-identity-api-impacts-gitlab-ee