مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Security Patch Advisory – GitLab CE/EE

Tracking #:432318289

Date:23-01-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed GitLab has released urgent security patch updates for both Community Edition (CE) and Enterprise Edition (EE) to remediate multiple high- and medium-severity vulnerabilities.

TECHNICAL DETAILS:

GitLab has released urgent security patch updates for both Community Edition (CE) and Enterprise Edition (EE) to remediate multiple high- and medium-severity vulnerabilities. These flaws expose affected GitLab installations to Denial of Service (DoS) attacks and, in one critical case, a potential two-factor authentication (2FA) bypass.

Vulnerability Details:

1. CVE-2025-13927 – Denial of Service in Jira Connect Integration

- Severity: High
- CVSS Score: 7.5
- Description:
  An unauthenticated attacker could send crafted requests with malformed authentication data to the Jira Connect integration, resulting in a denial of service condition.
- Impacted Versions: GitLab CE/EE: all versions from 11.9 before 18.6.4, 18.7 before 18.7.2, and 18.8 before 18.8.2

2. CVE-2025-13928 – Incorrect Authorization in Releases API

- Severity: High
- CVSS Score: 7.5
- Description:
  Improper authorization checks in the Releases API could allow an unauthenticated attacker to trigger a denial of service condition.
- Impacted Versions: GitLab CE/EE: all versions from 17.7 before 18.6.4, 18.7 before 18.7.2, and 18.8 before 18.8.2

3. CVE-2026-0723 – Two-Factor Authentication Bypass

- Severity: High
- CVSS Score: 7.4
- Description:
  An unchecked return value in authentication services could allow an attacker with prior knowledge of a victim's credential ID to bypass two-factor authentication by submitting forged device responses.
- Impacted Versions: GitLab CE/EE: all versions from 18.6 before 18.6.4, 18.7 before 18.7.2, and 18.8 before 18.8.2

4. CVE-2025-13335 – Infinite Loop in Wiki Redirects

- Severity: Medium
- CVSS Score: 6.5
- Description:
  Authenticated users could create malformed Wiki documents that bypass redirect cycle

detection, forcing GitLab into an infinite loop and causing a denial of service.
- Impacted Versions: GitLab CE/EE: all versions from 17.1 before 18.6.4, 18.7 before 18.7.2, and 18.8 before 18.8.2

5. CVE-2026-1102 – Denial of Service via SSH Authentication Requests

- Severity: Medium
- CVSS Score: 5.3
- Description:
  An unauthenticated attacker could cause a denial of service by repeatedly sending malformed SSH authentication requests.
- Impacted Versions: GitLab CE/EE: all versions from 12.3 before 18.6.4, 18.7 before 18.7.2, and 18.8 before 18.8.2

Fixed Versions

- GitLab 18.8.2, 18.7.2, or 18.6.4

RECOMMENDATIONS:

- Upgrade immediately to one of the patched versions
- Prioritize upgrades for internet-facing and mission-critical GitLab instances.

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://about.gitlab.com/releases/2026/01/21/patch-release-gitlab-18-8-2-released/