GitLab Patch Release: 18.10.1, 18.9.3, 18.8.7

Today, we are releasing versions 18.10.1, 18.9.3, 18.8.7 for GitLab Community Edition (CE) and Enterprise Edition (EE).

These versions contain important bug and security fixes, and we strongly recommend that all self-managed GitLab installations be upgraded to one of these versions immediately. GitLab.com is already running the patched version. GitLab Dedicated customers do not need to take action.

GitLab releases fixes for vulnerabilities in patch releases. There are two types of patch releases: scheduled releases and ad-hoc critical patches for high-severity vulnerabilities. Scheduled releases are released twice a month on the second and fourth Wednesdays. For more information, please visit our releases handbook and security FAQ. You can see all of GitLab release blog posts here.

For security fixes, the issues detailing each vulnerability are made public on our issue tracker 30 days after the release in which they were patched.

We are committed to ensuring that all aspects of GitLab that are exposed to customers or that host customer data are held to the highest security standards. To maintain good security hygiene, it is highly recommended that all customers upgrade to the latest patch release for their supported version. You can read more best practices in securing your GitLab instance in our blog post.

Recommended Action

We **strongly recommend** that all installations running a version affected by the issues described below are **upgraded to the latest version as soon as possible**.

When no specific deployment type (omnibus, source code, helm chart, etc.) of a product is mentioned, it means all types are affected.

Security fixes

Table of security fixes

Title	Severity
Improper Handling of Parameters issue in Jira Connect installations impacts GitLab CE/EE	High
Cross-Site Request Forgery issue in GLQL API impacts GitLab CE/EE	High
HTML Injection in vulnerability report impacts GitLab EE	High
Denial of Service issue in GraphQL API impacts GitLab CE/EE	High
Improper Access Control issue in WebAuthn 2FA impacts GitLab CE/EE	Medium
Improper Access Control issue in GraphQL query impacts GitLab EE	Medium
Denial of Service issue in CI configuration processing impacts GitLab CE/EE	Medium
Denial of Service issue in webhook configuration impacts GitLab CE/EE	Medium
Cross-site Scripting issue in Mermaid diagram renderer impacts GitLab CE/EE	Medium

Improper Access Control issue in Merge Requests impacts GitLab CE/EE	Medium
Access Control issue in GraphQL API impacts GitLab EE	Medium
Incorrect Authorization issue in authorization caching impacts GitLab EE	Low

CVE-2026-2370 - Improper Handling of Parameters issue in Jira Connect installations impacts GitLab CE/EE

GitLab has remediated an issue affecting Jira Connect installations that could have allowed an authenticated user with minimal workspace permissions to obtain installation credentials and impersonate the GitLab app due to improper authorization checks.

Impacted Versions: GitLab CE/EE: all versions from 14.3 before 18.8.7, 18.9 before 18.9.3, and 18.10 before 18.10.1
CVSS 8.1 (`CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N`)

Thanks maksyche for reporting this vulnerability through our HackerOne bug bounty program.

CVE-2026-3857 - Cross-Site Request Forgery issue in GLQL API impacts GitLab CE/EE

GitLab has remediated an issue that could have allowed an unauthenticated user to execute arbitrary GraphQL mutations on behalf of authenticated users due to insufficient CSRF protection.

Impacted Versions: GitLab CE/EE: all versions from 17.10 before 18.8.7, 18.9 before 18.9.3, and 18.10 before 18.10.1
CVSS 8.1 (`CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N`)

Thanks ahacker1 for reporting this vulnerability through our HackerOne bug bounty program.

CVE-2026-2995 - HTML Injection in vulnerability report impacts GitLab EE

GitLab has remediated an issue that could have allowed an authenticated user to add email addresses to targeted user accounts due to improper sanitization of HTML content.

Impacted Versions: GitLab EE: all versions from 15.4 before 18.8.7, 18.9 before 18.9.3, and 18.10 before 18.10.1
CVSS 7.7 (`CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:C/C:H/I:H/A:N`)

Thanks a_m_a_m and yvvdwf for reporting this vulnerability through our HackerOne bug bounty program.

CVE-2026-3988 - Denial of Service issue in GraphQL API impacts GitLab CE/EE

GitLab has remediated an issue that could have allowed an unauthenticated user to cause a denial of service by making the GitLab instance unresponsive due to improper input validation in GraphQL request processing.

Impacted Versions: GitLab CE/EE: all versions from 18.5 before 18.8.7, 18.9 before 18.9.3, and 18.10 before 18.10.1
CVSS 7.5 (`CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H`)

Thanks svalkanov for reporting this vulnerability through our HackerOne bug bounty program.

CVE-2026-2745 - Improper Access Control issue in WebAuthn 2FA impacts GitLab CE/EE

GitLab has remediated an issue that could have allowed an unauthenticated user to bypass WebAuthn two-factor authentication and gain unauthorized access to user accounts due to inconsistent input validation in the authentication process.

Impacted Versions: GitLab CE/EE: all versions from 7.11 before 18.8.7, 18.9 before 18.9.3, and 18.10 before 18.10.1
CVSS 6.8 (`CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:N`)

GitLab Docs

CVE-2026-1724 - Improper Access Control issue in GraphQL query impacts GitLab EE

GitLab has remediated an issue that could have allowed an unauthenticated user to access API tokens of self-hosted AI models due to improper access control.

Impacted Versions: GitLab EE: all versions from 18.5 before 18.8.7, 18.9 before 18.9.3, and 18.10 before 18.10.1
CVSS 6.8 (`CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N`)

Thanks maksyche for reporting this vulnerability through our HackerOne bug bounty program.

CVE-2025-13436 - Denial of Service issue in CI configuration processing impacts GitLab CE/EE

GitLab has remediated an issue that could have allowed an authenticated user to cause a denial of service due to excessive resource consumption when handling certain CI-related inputs.

Impacted Versions: GitLab CE/EE: all versions from 13.7 before 18.8.7, 18.9 before 18.9.3, and 18.10 before 18.10.1
CVSS 6.5 (`CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H`)

Thanks a92847865 for reporting this vulnerability through our HackerOne bug bounty program.

CVE-2025-13078 - Denial of Service issue in webhook configuration impacts GitLab CE/EE

GitLab has remediated an issue that could have allowed an authenticated user to cause a denial of service due to excessive resource consumption when processing certain webhook configuration inputs.

Impacted Versions: GitLab CE/EE: all versions from 16.10 before 18.8.7, 18.9 before 18.9.3, and 18.10 before 18.10.1
CVSS 6.5 (`CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H`)

Thanks lucky_luke for reporting this vulnerability through our HackerOne bug bounty program.

CVE-2026-2973 - Cross-site Scripting issue in Mermaid diagram renderer impacts GitLab CE/EE

GitLab has remediated an issue that could have allowed an authenticated user to execute arbitrary JavaScript in a user's browser due to improper sanitization of entity-encoded content in Mermaid diagrams.

Impacted Versions: GitLab CE/EE: all versions from 17.7 before 18.8.7, 18.9 before 18.9.3, and 18.10 before 18.10.1
CVSS 5.4 (`CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N`)

Thanks go7f0 for reporting this vulnerability through our HackerOne bug bounty program.

CVE-2026-2726 - Improper Access Control issue in Merge Requests impacts GitLab CE/EE

GitLab has remediated an issue that could have allowed an authenticated user to perform unauthorized actions on merge requests in other projects due to improper access control during cross-repository operations.

Impacted Versions: GitLab CE/EE: all versions from 11.10 before 18.8.7, 18.9 before 18.9.3, and 18.10 before 18.10.1
CVSS 4.3 (`CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N`)

Thanks pkkr for reporting this vulnerability through our HackerOne bug bounty program.

security category metadata and attributes in group security configuration due to improper access control.

Impacted Versions: GitLab EE: all versions from 18.6 before 18.8.7, 18.9 before 18.9.3, and 18.10 before 18.10.1
CVSS 4.3 (`CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N`)

Thanks kamikaze1337 for reporting this vulnerability through our HackerOne bug bounty program.

CVE-2026-4363 - Incorrect Authorization issue in authorization caching impacts GitLab EE

GitLab has remediated an issue that under certain conditions could have allowed an authenticated user to gain unauthorized access to resources due to improper caching of authorization decisions.

Impacted Versions: GitLab EE: all versions from 18.1 before 18.8.7, 18.9 before 18.9.3, and 18.10 before 18.10.1
CVSS 3.7 (`CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:L/I:L/A:N`)

This vulnerability was discovered internally by GitLab team member Fred de Gier.

Bug fixes

18.10.1

- Backport gocloud version and checksum fix to 18-10 stable
- [18.10] Zero downtime reindexing make setting async-durability optional
- Backport “CI: Update CNG mirror skip job regex”
- Backport of ‘Revert Code review flow automatic reviews enabled by default for groups’
- Backport Handle http-abort panic and pass http execution error
- Backport 18.10: Do not check column default in state machine initialization
- Backport of What’s new - 18.10
- [18.10 Backport] Fix statement timeouts on p_ci_job_artifacts during pipeline deletion
- Backport of “Execute BBM affected by single record table bug”
- Fix regression: “Git operations for Deploy keys fail on a Geo Site”

18.9.3

- Backport gocloud version and checksum fix to 18-9 stable
- [Backport 18.9] Fix gitlab:setup failure on fresh database
- [18.9] Update dependency oj to v3.16.15
- Backport of ‘Use v-safe-html for commit.titleHtml in collapsible commit info’
- 18.9 Backport of ‘Fix re-archiving projects and subgroups after group unarchive’
- Backport of ‘Fix edit in pipeline editor button not showing on ci file on file navigation’
- [18.9] GLQL advanced finder, remove project_ids
- Backport of ‘Update rack gem to 2.2.22’
- Backport `oj` and `oj-introspect` gem updates
- [18.9] Exclude group-covered projects from search authorization to reduce redundant payload
- Backport “CI: Update CNG mirror skip job regex”
- [18.9] Zero downtime reindexing make setting async-durability optional
- Backport 18.9: Do not check column default in state machine initialization

- Fix regression: “Git operations for Deploy keys fail on a Geo Site”
- Backport: Fix Valkey version detection
- 18.9 Backport CI: Fix the package install for zypper based distros
- [18.9] Backport Mattermost Security Updates February 23, 2026
- Backport 18-9-stable - check-packages uses Pulp

18.8.7

- Fix command execution race condition in Agentic Chat
- Backport of ‘fix: allow explain for all add ons’
- [18.8] Update dependency oj to v3.16.15
- 18.8 Backport of ‘Fix re-archiving projects and subgroups after group unarchive’
- Add DAP self-hosted model DAP check in user_authorizable
- Backport of ‘Fix edit in pipeline editor button not showing on ci file on file navigation’
- [18.8] GLQL advanced finder, remove project_ids
- Backport `oj` and `oj-introspect` gem updates
- Backport of ‘Update rack gem to 2.2.22’
- Backport “CI: Update CNG mirror skip job regex”
- [18.8] Exclude group-covered projects from search authorization to reduce redundant payload
- [18.8] Zero downtime reindexing make setting async-durability optional
- Backport of “Execute BBM affected by single record table bug”
- [18.8 Backport] Fix statement timeouts on p_ci_job_artifacts during pipeline deletion
- Fix regression: “Git operations for Deploy keys fail on a Geo Site”
- 18.8 Backport CI: Fix the package install for zypper based distros
- [18.8] Backport Mattermost Security Updates February 23, 2026
- Backport 18-8-stable - check-packages uses Pulp

Important notes on upgrading

The SLES 12.5 package is not available for GitLab 18.10.1.

This patch includes database migrations that may impact your upgrade process.

Impact on your installation:

- **Single-node instances**: This patch will cause downtime during the upgrade as migrations must complete before GitLab can start.
- **Multi-node instances**: With proper zero-downtime upgrade procedures, this patch can be applied without downtime.

Post-deploy migrations

The following versions include post-deploy migrations that can run after the upgrade:

- 18.10.1
- 18.9.3
- 18.8.7

To learn more about the impact of upgrades on your installation, see:

GitLab Docs

Updating

To update GitLab, see the Update page. To update GitLab Runner, see the Updating the Runner page.

Receive Patch Notifications

To receive patch blog notifications delivered to your inbox, visit our contact us page. To receive release notifications via RSS, subscribe to our patch release RSS feed or our RSS feed for all releases.