GitLab Patch Release: 18.11.1, 18.10.4, 18.9.6

On April 22, 2026, we released versions 18.11.1, 18.10.4, 18.9.6 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
Cross-Site Request Forgery issue in GraphQL API impacts GitLab CE/EE	High
Improper Resolution of Path Equivalence issue in Web IDE asset impacts GitLab CE/EE	High
Cross-site Scripting issue in Storybook impacts GitLab CE/EE	High
Denial of Service issue in discussions endpoint impacts GitLab CE/EE	Medium
Denial of Service issue in Jira import impacts GitLab CE/EE	Medium
Denial of Service issue in notes endpoint impacts GitLab CE/EE	Medium
Denial of Service issue in GraphQL API impacts GitLab CE/EE	Medium
Insufficient Session Expiration issue in virtual registry credentials validation impacts GitLab CE/EE	Medium

Improper Access Control issue in issue description renderer impacts GitLab CE/EE	Medium
Improper Restriction of Rendered UI Layers or Frames issue in Mermaid sandbox impacts GitLab CE/EE	Low
Improper Access Control issue in project fork relationship API impacts GitLab CE/EE	Low

CVE-2026-4922 - Cross-Site Request Forgery issue in GraphQL API impacts GitLab CE/EE

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

Impacted Versions: GitLab CE/EE: all versions from 17.0 before 18.9.6, 18.10 before 18.10.4, and 18.11 before 18.11.1
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-2026-5816 - Improper Resolution of Path Equivalence issue in Web IDE asset impacts GitLab CE/EE

GitLab has remediated an issue that could have allowed an unauthenticated user to execute arbitrary JavaScript in a user's browser session due to improper path validation under certain conditions.

Impacted Versions: GitLab CE/EE: all versions from 18.10 before 18.10.4 and 18.11 before 18.11.1
CVSS 8.0 (`CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:N`)

Thanks joaxcar for reporting this vulnerability through our HackerOne bug bounty program

CVE-2026-5262 - Cross-site Scripting issue in Storybook impacts GitLab CE/EE

GitLab has remediated an issue that under certain conditions could have allowed an unauthenticated user to access tokens in the Storybook development environment due to improper input validation.

Impacted Versions: GitLab CE/EE: all versions from 16.1 before 18.9.6, 18.10 before 18.10.4, and 18.11 before 18.11.1
CVSS 8.0 (`CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:N`)

Thanks joaxcar for reporting this vulnerability through our HackerOne bug bounty program

CVE-2025-0186 - Denial of Service issue in discussions endpoint impacts GitLab CE/EE

GitLab has remediated an issue that could have allowed an authenticated user to cause denial of service under certain conditions by exhausting server resources by making crafted requests to a discussions endpoint.

Impacted Versions: GitLab CE/EE: all versions from 10.6 before 18.9.6, 18.10 before 18.10.4, and 18.11 before 18.11.1
CVSS 6.5 (`CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H`)

Thanks pwnie for reporting this vulnerability through our HackerOne bug bounty program

CVE-2026-1660 - Denial of Service issue in Jira import impacts GitLab CE/EE

GitLab has remediated an issue that under certain conditions could have allowed an authenticated user to cause denial of service when importing issues due to improper input validation.

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

CVE-2025-6016 - Denial of Service issue in notes endpoint impacts GitLab CE/EE

GitLab has remediated an issue that could have allowed an authenticated user to cause denial of service due to insufficient resource allocation limits when retrieving notes under certain conditions.

Impacted Versions: GitLab CE/EE: all versions from 9.2 before 18.9.6, 18.10 before 18.10.4, and 18.11 before 18.11.1
CVSS 6.5 (`CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H`)

Thanks pwnie for reporting this vulnerability through our HackerOne bug bounty program

CVE-2025-3922 - Denial of Service issue in GraphQL API impacts GitLab CE/EE

GitLab has remediated an issue that could have allowed an authenticated user to cause denial of service by overwhelming system resources under certain conditions due to insufficient resource allocation limits in the GraphQL API.

Impacted Versions: GitLab CE/EE: all versions from 12.4 before 18.9.6, 18.10 before 18.10.4, and 18.11 before 18.11.1
CVSS 6.5 (`CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H`)

Thanks pwnie for reporting this vulnerability through our HackerOne bug bounty program

CVE-2026-6515 - Insufficient Session Expiration issue in virtual registry credentials validation impacts GitLab CE/EE

GitLab has remediated an issue that could have allowed a user to use invalidated or incorrectly scoped credentials to access Virtual Registries under certain conditions.

Impacted Versions: GitLab CE/EE: all versions from 18.2 before 18.9.6, 18.10 before 18.10.4, and 18.11 before 18.11.1
CVSS 5.4 (`CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N`)

This vulnerability has been discovered internally by GitLab team member David Fernandez

CVE-2026-5377 - Improper Access Control issue in issue description renderer impacts GitLab CE/EE

GitLab has remediated an issue that could have allowed an authenticated user to access titles of confidential or private issues in public projects due to improper access control in the issue description rendering process.

Impacted Versions: GitLab CE/EE: all versions from 18.11 before 18.11.1
CVSS 4.3 (`CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N`)

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

CVE-2026-3254 - Improper Restriction of Rendered UI Layers or Frames issue in Mermaid sandbox impacts GitLab CE/EE

GitLab has remediated an issue that under certain conditions could have allowed an authenticated user to load unauthorized content into another user's browser due to improper input validation in the Mermaid sandbox.

Impacted Versions: GitLab CE/EE: all versions from 18.11 before 18.11.1
CVSS 3.5 (`CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:L/A:N`)

Thanks joaxcar for reporting this vulnerability through our HackerOne bug bounty program

GitLab has remediated an issue that under certain conditions could have allowed an authenticated user with project owner permissions to bypass group fork prevention settings due to improper authorization checks.

Impacted Versions: GitLab CE/EE: all versions from 11.2 before 18.9.6, 18.10 before 18.10.4, and 18.11 before 18.11.1
CVSS 2.7 (`CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:N`)

Thanks theluci for reporting this vulnerability through our HackerOne bug bounty program

Bug fixes

18.11.1

- Backport- Use force_index_repo task type for Zoekt schema_version bump reindexing
- Backport docs: Update PostgreSQL version documentation for PG17
- [18.11] Skip re-creating of constraint when migration spec is skipped
- Backport of " 18.11 What's new"
- Revert "Merge branch 'renovate-ci-templates/auto-build-image-4.x' into 'v18.11.0-ee'"
- Backport of "BBM - Skip 3 migrations referencing dropped tables"
- [18.11] Fix session ID dropdown never appearing during active agentic chat
- Backport of 'Fix JSON tables with non-string values'
- 18.11 - Cherry-pick !9288 and !9311 - Remove PackageCloud CI and rename pulp jobs
- Backport of 'Remove package OS check from deployer task' - 18.11

18.10.4

- [18.10] Scope start-rails-specs changes rule to MR pipelines
- Backport of 'Fix runner token reset returning 500 for unassigned project runners' to 18.10
- Backport of 'Fix flaky new_project_spec.rb by scoping within pane'
- 18.10 Backport of 'Update rack to 2.2.23'
- Backport of "Skip BBMs referencing dropped tables in single-record bug retry"
- Backport of Added reload to address flaky pipeline spec race condition
- Backport GITLAB_ZOEKT_INDEXER v1.11.1
- Backport of Fix flaky tests for ui_variable_non_inheritable_when_forward_pipeline_variables_false_spec
- Backport of 'Skip CI finished builds backfill when ClickHouse is not configured'
- Backport to 18.10: Geo: Run concurrency limit worker on secondary sites
- Backport of 'Geo: Switch blob download to use GitLab::HTTP to avoid llhttp-ffi issue'
- Backport of Release environment deploy needs Omnibus package - 18.10
- Backport- Use force_index_repo task type for Zoekt schema_version bump reindexing
- Backport of add feature flag to gate default Sidekiq concurrency limit calculation
- [18.10] Skip re-creating of constraint when migration spec is skipped
- Docs backport: Add note about Agent Platform flow configurations not available until 18.11
- Backport of praba/release-connections-from-all-hosts and stomlinson/feature-check-dead-connections to 18.10
- Backport to 18.10: Geo: Fix site validation when outbound request filtering is enabled
- Ensure postgresql_new is included in GitLab CE
- 18.10 backport of 'Update rack to 2.2.23'

- Backport: fix: Set sv timeout when restarting Gitaly to 18.10
- [18.10] Remove Mattermost for SLES-12.5
- 18.10 - Cherry-pick !9288 and !9311 - Remove PackageCloud CI and rename pulp jobs
- Backport of 'Remove package OS check from deployer task' - 18.10

18.9.6

- chore: bump gitlab-zoekt to v1.8.2 on 18-9-stable
- [18.9] Scope start-rails-specs changes rule to MR pipelines
- 18.9 Backport of 'update zlib to 3.2.3'
- Backport to 18.9: Geo: Run concurrency limit worker on secondary sites
- Backport of Release environment deploy needs Omnibus package - 18.9
- Backport- Use force_index_repo task type for Zoekt schema_version bump reindexing
- [18.9] Skip re-creating of constraint when migration spec is skipped
- Docs backport: Add note about Agent Platform flow configurations not available until 18.11
- Backport of add feature flag to gate default Sidekiq concurrency limit calculation
- Backport GITLAB_ZOEKT_INDEXER v1.8.2
- Backport to 18.9: Geo: Fix site validation when outbound request filtering is enabled
- Backport: Ensure postgresql_new is included in GitLab CE
- 18.9 backport of 'Update rack to 2.2.23'
- Upgrade postgresql-17 to 17.8 for 18-9-stable
- Upgrade postgresql-16 to 16.13 for 18-9-stable
- Backport: fix: Set sv timeout when restarting Gitaly to 18.9
- [18.9] Remove Mattermost for SLES-12.5
- 18.9 - Cherry-pick !9288 and !9311 - Remove PackageCloud CI and rename pulp jobs
- Remove .gitlab folder under package gitlab-rails
- Backport of 'Remove package OS check from deployer task' - 18.9

Important notes on upgrading

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.

Regular migrations

The following versions include regular migrations that run during the upgrade process:

- 18.11.1
- 18.10.4
- 18.9.6

- 18.11.1
- 18.10.4

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

- Zero-downtime upgrades for multi-node deployments
- Standard upgrades for single-node installations

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,