GitLab Patch Release: 18.7.1, 18.6.3, 18.5.5

On January 7, 2026, we released versions 18.7.1, 18.6.3, 18.5.5 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
Stored Cross-site Scripting issue in GitLab Flavored Markdown placeholders impacts GitLab CE/EE	High
Cross-site scripting issue in Web IDE impacts GitLab CE/EE	High
Missing Authorization issue in Duo Workflows API impacts GitLab EE	High
Denial of Service issue in import functionality impacts GitLab CE/EE	Medium
Missing Authorization issue in AI GraphQL mutation impacts GitLab EE	Medium
Insufficient Access Control Granularity issue in GraphQL runnerUpdate mutation impacts GitLab CE/EE	Medium
Information Disclosure issue in Mermaid diagram rendering impacts GitLab CE/EE	Low

GitLab has remediated an issue that could have allowed an authenticated user to achieve stored cross-site scripting by exploiting GitLab Flavored Markdown placeholder processing.

Impacted Versions: GitLab CE/EE: all versions from 18.2.2 before 18.5.5, 18.6 before 18.6.3, and 18.7 before 18.7.1
CVSS 8.7 (`CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:N`)

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

CVE-2025-13761 - Cross-site Scripting issue in Web IDE impacts GitLab CE/EE

GitLab has remediated an issue that could have allowed an unauthenticated user to execute arbitrary code in the context of an authenticated user's browser by convincing the legitimate user to visit a specially crafted webpage.

Impacted Versions: GitLab CE/EE: all versions from 18.6 before 18.6.3, and 18.7 before 18.7.1
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-2025-13772 - Missing Authorization issue in Duo Workflows API impacts GitLab EE

GitLab has remediated an issue that could have allowed an authenticated user to access and utilize AI model settings from unauthorized namespaces by manipulating namespace identifiers in API requests.

Impacted Versions: GitLab EE: all versions from 18.4 before 18.5.5, 18.6 before 18.6.3, and 18.7 before 18.7.1
CVSS 7.1 (`CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N`)

This vulnerability has been discovered internally by GitLab team member Jessie Young.

CVE-2025-13781 - Missing Authorization issue in AI GraphQL mutation impacts GitLab EE

GitLab has remediated an issue that could have allowed an authenticated user to modify instance-wide AI feature provider settings by exploiting missing authorization checks in GraphQL mutations.

Impacted Versions: GitLab EE: all versions from 18.5 before 18.5.5, 18.6 before 18.6.3, and 18.7 before 18.7.1
CVSS 6.5 (`CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N`)

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

CVE-2025-10569 - Denial of Service issue in import functionality impacts GitLab CE/EE

GitLab has remediated an issue that could have allowed authenticated users to create a denial of service condition by providing crafted responses to external API calls.

Impacted Versions: GitLab CE/EE: all versions from 8.3 before 18.5.5, 18.6 before 18.6.3, and 18.7 before 18.7.1
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.

GitLab has remediated an issue that could have allowed authenticated users with specific permissions to remove all project runners from unrelated projects by manipulating GraphQL runner associations.

Impacted Versions: GitLab CE/EE: all versions from 15.4 before 18.5.5, 18.6 before 18.6.3, and 18.7 before 18.7.1
CVSS 5.4 (`CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:L`)

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

CVE-2025-3950 - Information Disclosure issue in Mermaid diagram rendering impacts GitLab CE/EE

GitLab has remediated an issue that could have allowed a user to leak sensitive connection information by referencing specially crafted images that bypass asset proxy protection.

Impacted Versions: GitLab CE/EE: all versions from 10.3 before 18.5.5, 18.6 before 18.6.3, and 18.7 before 18.7.1
CVSS 3.5 (`CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N`)

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

Update Libpng version to 1.6.51

Libpng has been updated to version 1.6.51, which contains fixes for security vulnerabilities including CVE-2025-65018 and CVE-2025-64720.

Bug fixes

18.7.1

- Backport of 'Revert Merge branch '582543-opinionated-duo-chat-focus' into 'master''
- Backport of Add CI builds metadata migration configuration to 18.7 upgrade notes
- Backport of "Don't try to return connections to the pool early in a web request"
- Backport of "Clear the query cache when releasing load balancing hosts"
- Backport "Fix version-skipping upgrade blocker for namespace traversal IDs backfill"
- Backport of 'Fix Elasticsearch pagination with null sortable field values'
- [Backport 18.7] No-op BackfillSlackIntegrationsScopesShardingKey BBM
- Backport of 'Wrap merge_data & merge_request into single transaction'
- Backport of 'Resolve GraphQL type mismatch in Cleanup policy type'
- Backport of 'Fix 404 errors for Duo Workflow WS connection'

18.6.3

- Log truncation to 18-6 stable branch
- Backport of 'Add status filter argument to work items CSV export'
- Backport 'tskorupa/fix-check_e82ff70482-constraint-validation' into '18-6-stable-ee'
- Backport of Add pipeline_per_user rate limit
- Backport of Dependency export fix
- 18.6 Backport: "Add type handling for findings with locations saved as Strings"
- Backport: Improve handling of attachment urls and filenames, fix undercoverage 18-6
- Backport of Fix content and content-type mismatch in files e2e test

- Backport of: Handle updated Jira API calls to permit Jira issue imports again
- Backport of Fix scan execution policy overriding YAML variables
- Backport (18.6): Update dependency @gitlab/web-ide to ^0.0.1-dev-20251210140521
- Backport of 'Workhorse: use upstream for DWS API requests'
- Backport 'Allow ClickHouse migrations to be skipped'
- Backport "Fix version-skipping upgrade blocker for namespace traversal IDs backfill"
- Backport of 'Fix Elasticsearch pagination with null sortable field values'
- [18.6] Backport Mattermost Security Updates November 21, 2025
- [Backport - 18-6-stable] Disable allow_failure for the check-packages-functionality job in the tag pipelines
- Backport of 'Fix 404 errors for Duo Workflow WS connection'

18.5.5

- Backport: Improve handling of attachment urls and filenames, fix undercoverage 18-5
- Backport of 'Handle 429s during github LFS import'
- Backport of Dependency export fix
- Backport of 'Add status filter argument to work items CSV export'
- 18.5 Backport: "Add type handling for findings with locations saved as Strings"
- Backport of Fix content and content-type mismatch in files e2e test
- [Backport 18.5] Exclude Git HTTP requests from authenticated web throttle
- Backport of: Handle updated Jira API calls to permit Jira issue imports again
- Backport(18.5): Update dependency @gitlab/web-ide to ^0.0.1-dev-20251210140521
- Backport of 'Workhorse: use upstream for DWS API requests'
- [Backport - 18-5-stable] Disable allow_failure for the check-packages-functionality job in the tag pipelines
- Backport of 'Fix 404 errors for Duo Workflow WS connection'

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.

Post-deploy migrations

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

- 18.7.1
- 18.6.3

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

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

Receive Patch Notifications