← Back to releases (/releases/categories/releases/)

Nov 12, 2025 - Félix Veillette-Potvin (/company/team/#gitlab) (https://gitlab.com/fvpotvin) (https://twitter.com/gitlab)

GitLab Patch Release: 18.5.2, 18.4.4, 18.3.6

Learn more about GitLab Patch Release: 18.5.2, 18.4.4, 18.3.6 for GitLab Community Edition (CE) and Enterprise Edition (EE).

Today, we are releasing versions 18.5.2, 18.4.4, 18.3.6 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 (https://handbook.gitlab.com/handbook/engineering/releases/) and security FAQ (https://about.gitlab.com/security/faq/). You can see all of GitLab release blog posts here (/releases/categories/releases/).

For security fixes, the issues detailing each vulnerability are made public on our issue tracker (https://gitlab.com/gitlab-org/gitlab/-/issues/?sort=created_date&state=closed&label_name%5B%5D=bug%3A%3Avulnerability&confidential=no&first_page_size=100) 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 (/blog/2020/05/20/gitlab-instance-security-best-practices/) 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 scripting issue in k8s proxy impacts GitLab CE/EE	High
Incorrect Authorization issue in workflows impacts GitLab EE	Medium
Information Disclosure issue in GraphQL subscriptions impacts GitLab CE/EE	Medium
Information Disclosure issue in access control impacts GitLab CE/EE	Medium
Prompt Injection issue in GitLab Duo review impacts GitLab EE	Low
Information Disclosure issue in packages API endpoint impacts GitLab CE/EE	Low
Client Side Path Traversal issue in branch names impacts GitLab EE	Low
Improper Access Control issue in GitLab Pages impacts GitLab CE/EE	Low
Denial of service issue in markdown impacts GitLab CE/EE	Low

CVE-2025-11224 (https://www.cve.org/CVERecord?id=CVE-2025-11224) - Cross-site scripting issue in k8s proxy impacts GitLab CE/EE

GitLab has remediated an issue that, under certain conditions, could have allowed an authenticated user to execute stored cross-site scripting through improper input validation in the Kubernetes proxy functionality.

Impacted Versions: GitLab CE/EE: all versions from 15.10 before 18.3.6, 18.4 before 18.4.4, and 18.5 before 18.5.2
CVSS 7.7 (`CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:C/C:H/I:H/A:N` (https://gitlab-com.gitlab.io/gl-security/product-security/appsec/cvss-calculator/explain#explain=CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:C/C:H/I:H/A:N))

Thanks joaxcar (https://hackerone.com/joaxcar) for reporting this vulnerability through our HackerOne bug bounty program

CVE-2025-11865 (https://www.cve.org/CVERecord?id=CVE-2025-11865) - Incorrect Authorization issue in workflows impacts GitLab EE

GitLab has remediated an issue that, under certain circumstances, could have allowed a user to remove Duo flows of another user.

Impacted Versions: GitLab EE: all versions from 18.1 before 18.3.6, 18.4 before 18.4.4, and 18.5 before 18.5.2
CVSS 6.5 (`CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N` (https://gitlab-com.gitlab.io/gl-security/product-security/appsec/cvss-calculator/explain#explain=CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N))

This vulnerability has been discovered internally by GitLab team member Dylan Griffith (https://gitlab.com/DylanGriffith).

CVE-2025-2615 (https://www.cve.org/CVERecord?id=CVE-2025-2615) - Information Disclosure issue in GraphQL subscriptions impacts GitLab CE/EE

GitLab has remediated an issue that could have allowed a blocked user to access sensitive information by establishing GraphQL subscriptions through WebSocket connections.

Impacted Versions: GitLab CE/EE: all versions from 16.7 before 18.3.6, 18.4 before 18.4.4, and 18.5 before 18.5.2
CVSS 4.3 (`CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N` (https://gitlab-com.gitlab.io/gl-security/product-security/appsec/cvss-calculator/explain#explain=CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N))

Thanks rogerace (https://hackerone.com/rogerace) for reporting this vulnerability through our HackerOne bug bounty program.

CVE-2025-7000 (https://www.cve.org/CVERecord?id=CVE-2025-7000) - Information Disclosure issue in access control impacts GitLab CE/EE

GitLab has remdiated an issue in GitLab CE/EE that under specific conditions, could have allowed unauthorized users to view confidential branch names by accessing project issues with related merge requests.

Impacted Versions: GitLab CE/EE: all versions from 17.6 before 18.3.6, 18.4 before 18.4.4, and 18.5 before 18.5.2
CVSS 4.3 (`CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N` (https://gitlab-com.gitlab.io/gl-security/product-security/appsec/cvss-calculator/explain#explain=CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N))

Thanks weasterhacker (https://hackerone.com/weasterhacker) for reporting this vulnerability through our HackerOne bug bounty program

CVE-2025-6945 (https://www.cve.org/CVERecord?id=CVE-2025-6945) - Prompt Injection issue in GitLab Duo review impacts GitLab EE

GitLab has remediated an issue that could have allowed an authenticated user to leak sensitive information from confidential issues by injecting hidden prompts in merge request comments.

Impacted Versions: GitLab EE: all versions from 17.9 before 18.3.6, 18.4 before 18.4.4, and 18.5 before 18.5.2
CVSS 3.5 (`CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N` (https://gitlab-com.gitlab.io/gl-security/product-security/appsec/cvss-calculator/explain#explain=CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N))

Thanks rogerace (https://hackerone.com/rogerace) for reporting this vulnerability through our HackerOne bug bounty program

CVE-2025-11990 (https://www.cve.org/CVERecord?id=CVE-2025-11990) - Client Side Path Traversal issue in branch names impacts GitLab EE

GitLab has remediated an issue that could have allowed an authenticated user to gain CSRF tokens by exploiting improper input validation in repository references combined with redirect handling weaknesses.

Impacted Versions: GitLab EE: all versions from 18.4 before 18.4.4, and 18.5 before 18.5.2
CVSS 3.1 (`CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N` (https://gitlab-com.gitlab.io/gl-security/product-security/appsec/cvss-calculator/explain#explain=CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N))

Thanks swiftee (https://hackerone.com/swiftee) for reporting this vulnerability through our HackerOne bug bounty program

CVE-2025-6171 (https://www.cve.org/CVERecord?id=CVE-2025-6171) - Information Disclosure issue in packages API endpoint impacts GitLab CE/EE

GitLab has remediated an issue that could have allowed an authenticated user with reporter access to view branch names and pipeline details by accessing the packages API endpoint even when repository access was disabled.

Impacted Versions: GitLab CE/EE: all versions from 13.2 before 18.3.6, 18.4 before 18.4.4, and 18.5 before 18.5.2
CVSS 3.1 (`CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N` (https://gitlab-com.gitlab.io/gl-security/product-security/appsec/cvss-calculator/explain#explain=CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N))

Thanks iamgk808 (https://hackerone.com/iamgk808) for reporting this vulnerability through our HackerOne bug bounty program

CVE-2025-7736 (https://www.cve.org/CVERecord?id=CVE-2025-7736) - Improper Access Control issue in GitLab Pages impacts GitLab CE/EE

GitLab has remediated an issue that could have allowed an authenticated user to bypass access control restrictions and view GitLab Pages content intended only for project members by authenticating through OAuth providers.

Impacted Versions: GitLab CE/EE: all versions from 17.9 before 18.3.6, 18.4 before 18.4.4, and 18.5 before 18.5.2
CVSS 3.1 (`CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N` (https://gitlab-com.gitlab.io/gl-security/product-security/appsec/cvss-calculator/explain#explain=CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N))

Thanks mateuszek (https://hackerone.com/mateuszek) for reporting this vulnerability through our HackerOne bug bounty program

CVE-2025-12983 (https://www.cve.org/CVERecord?id=CVE-2025-12983) - Denial of service issue in markdown impacts GitLab CE/EE

GitLab has remediated an issue that could have allowed an authenticated user to cause a denial of service condition by submitting specially crafted markdown content with nested formatting patterns.

Impacted Versions: GitLab CE/EE: all versions from 16.9 before 18.3.6, 18.4 before 18.4.4, and 18.5 before 18.5.2
CVSS 3.1 (`CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:L` (https://gitlab-com.gitlab.io/gl-security/product-security/appsec/cvss-

calculator/explain#explain=CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:L))

Thanks phli (https://hackerone.com/phli) for reporting this vulnerability through our HackerOne bug bounty program

libxslt security updates

libxslt has been updated to version 1.1.43 which contains fixes for security vulnerabilities including CVE-2024-55549 and CVE-2025-24855

Bug fixes

18.5.2

- [18.5] Backport of "Rails: Add explicit ClickHouse check skip" (https://gitlab.com/gitlab-org/build/CNG/-/merge_requests/2687)
- Backport of 'rf-disable-sec-attribute-feature-flags' (https://gitlab.com/gitlab-org/gitlab/-/merge_requests/209319)
- Backport E2E test: fix create project web ui 18-5 (https://gitlab.com/gitlab-org/gitlab/-/merge_requests/209855)
- 18.5 Backport of 'Fix query for finding existing Jira issues for vulnerabilities' (https://gitlab.com/gitlab-org/gitlab/-/merge_requests/209249)
- Backport of 'Filter out group-level rules from details page' (https://gitlab.com/gitlab-org/gitlab/-/merge_requests/209757)
- [18.5] Reduce cached SQL queries in `/api/v4/internal/pages` endpoint (https://gitlab.com/gitlab-org/gitlab/-/merge_requests/210364)
- [18.5] Update dependency openssl to v3.3.2 (https://gitlab.com/gitlab-org/gitlab/-/merge_requests/210400)
- Update dependency simplecov-cobertura to v3 (https://gitlab.com/gitlab-org/gitlab/-/merge_requests/210610)
- Backport of Fix password validation exception for FIPS (https://gitlab.com/gitlab-org/gitlab/-/merge_requests/209795)
- Backport of 'Fix admin_project_member policy for SAML projects related to user namespaces' (https://gitlab.com/gitlab-org/gitlab/-/merge_requests/210300)
- Backport of 'Web Agentic Chat: fix calling workflowGoal on undefined' (https://gitlab.com/gitlab-org/gitlab/-/merge_requests/210536)
- [Backport 18.5] Turn off Duo core widget for self-managed (https://gitlab.com/gitlab-org/gitlab/-/merge_requests/210353)
- Backport of 'Fix status mapping evaluation for non-persisted current status records' (https://gitlab.com/gitlab-org/gitlab/-/merge_requests/210747)
- [18.5] Upgrade Rack to 2.2.20 (https://gitlab.com/gitlab-org/gitlab/-/merge_requests/210341)
- Backport of Elastic rake tasks projects_not_indexed and index_projects_status could be confusing (https://gitlab.com/gitlab-org/gitlab/-/merge_requests/210737)

- Backport of 'Add deleted Geo migration back' (https://gitlab.com/gitlab-org/gitlab/-/merge_requests/210512)
- Backport of Allow Legacy FIPS instances to Upgrade Oauth secerets (https://gitlab.com/gitlab-org/gitlab/-/merge_requests/211228)
- Backport of Zoekt Exclude forks and Include archived filters in the cache key (https://gitlab.com/gitlab-org/gitlab/-/merge_requests/210726)
- [Backport 18.5] Clear tracking queues when recreating index from scratch (https://gitlab.com/gitlab-org/gitlab/-/merge_requests/211436)
- [18.5 Backport] Delete failed reindexing indexes created over 30 days ago (https://gitlab.com/gitlab-org/gitlab/-/merge_requests/211435)
- Backport of 'Fix redirect loop in Gitea rate limit` (https://gitlab.com/gitlab-org/gitlab/-/merge_requests/211412)
- [18.5 Backport] Set http_continue_timeout to nil for s3 client (https://gitlab.com/gitlab-org/gitlab/-/merge_requests/211537)
- [18.5] Fix background migration when Ghost user is missing (https://gitlab.com/gitlab-org/gitlab/-/merge_requests/211571)
- Backport Support Jira Cloud and Server issue fetching (https://gitlab.com/gitlab-org/gitlab/-/merge_requests/211409)
- [18.5] Fix test failure by adjusting dates to match partition range (https://gitlab.com/gitlab-org/gitlab/-/merge_requests/211708)
- Backport 'Revert merge trains changes to getState GraphQL query' (https://gitlab.com/gitlab-org/gitlab/-/merge_requests/211556)
- Backport 'Update merge request widget polling timeout intervals' (https://gitlab.com/gitlab-org/gitlab/-/merge_requests/211750)
- [18.5] Downgrade Zeitwerk to 2.6.18 (https://gitlab.com/gitlab-org/gitlab/-/merge_requests/211524)
- [Backport/18.5] of Fix instance bbm for mishandled nil verification token (https://gitlab.com/gitlab-org/gitlab/-/merge_requests/210558)
- Fix NGINX not routing traffic to the right server (https://gitlab.com/gitlab-org/omnibus-gitlab/-/merge_requests/8808)
- [18.5] Uninstall rexml 3.4.0 and ensure 3.4.4 is used (https://gitlab.com/gitlab-org/omnibus-gitlab/-/merge_requests/8814)
- Update redis to v7.2.11 (https://gitlab.com/gitlab-org/omnibus-gitlab/-/merge_requests/8820)
- Bump eventmachine-tail gem to version 0.6.6 (https://gitlab.com/gitlab-org/omnibus-gitlab/-/merge_requests/8836)
- [18.5] Upgrade Rack to 2.2.20 (https://gitlab.com/gitlab-org/omnibus-gitlab/-/merge_requests/8849)

18.4.4

- [18.4] Backport of "Rails: Add explicit ClickHouse check skip" (https://gitlab.com/gitlab-org/build/CNG/-/merge_requests/2688)
- [18.4] Reduce cached SQL queries in `/api/v4/internal/pages` endpoint (https://gitlab.com/gitlab-org/gitlab/-/merge_requests/210365)
- [18.4] Update dependency openssl to v3.3.2 (https://gitlab.com/gitlab-org/gitlab/-/merge_requests/210402)

- Backports branch 'tachyons-remove-ff-sha512-oauth' into 'master' (https://gitlab.com/gitlab-org/gitlab/-/merge_requests/208305)
- [18.4] Update rexml to v3.4.4 (https://gitlab.com/gitlab-org/gitlab/-/merge_requests/210395)
- Backport of Fix password validation exception for FIPS (https://gitlab.com/gitlab-org/gitlab/-/merge_requests/209793)
- Backport of 'Fix admin_project_member policy for SAML projects related to user namespaces' (https://gitlab.com/gitlab-org/gitlab/-/merge_requests/210295)
- [Backport 18.4] Turn off Duo core widget for self-managed (https://gitlab.com/gitlab-org/gitlab/-/merge_requests/210361)
- [18.4] Upgrade Rack to 2.2.20 (https://gitlab.com/gitlab-org/gitlab/-/merge_requests/210343)
- Backport of Elastic rake tasks projects_not_indexed and index_projects_status could be confusing (https://gitlab.com/gitlab-org/gitlab/-/merge_requests/210754)
- Backport of 'Add deleted Geo migration back' (https://gitlab.com/gitlab-org/gitlab/-/merge_requests/210510)
- Backport of 'Fix: prevent duplicate '?' in Download directory URL (use '&' for extra params)' (https://gitlab.com/gitlab-org/gitlab/-/merge_requests/210925)
- Backport of Allow Legacy FIPS instances to Upgrade Oauth secrets (https://gitlab.com/gitlab-org/gitlab/-/merge_requests/211227)
- Backport of 'Fix redirect loop in Gitea rate limit' (https://gitlab.com/gitlab-org/gitlab/-/merge_requests/211421)
- [18.4 Backport] Set http_continue_timeout to nil for s3 client (https://gitlab.com/gitlab-org/gitlab/-/merge_requests/211538)
- Backport of Update Jira integration to use token-based pagination and Support Jira Cloud and Server issue fetching (https://gitlab.com/gitlab-org/gitlab/-/merge_requests/211563)
- Backport 'Revert merge trains changes to getState GraphQL query' (https://gitlab.com/gitlab-org/gitlab/-/merge_requests/211555)
- Backport of Zoekt Exclude forks and Include archived filters in the cache key (https://gitlab.com/gitlab-org/gitlab/-/merge_requests/210729)
- Backport 'Update merge request widget polling timeout intervals' (https://gitlab.com/gitlab-org/gitlab/-/merge_requests/211751)
- [Backport/18.4] of Fix instance bbm for mishandled nil verification token (https://gitlab.com/gitlab-org/gitlab/-/merge_requests/210555)
- [18.4] Uninstall rexml 3.4.0 and ensure 3.4.4 is used (https://gitlab.com/gitlab-org/omnibus-gitlab/-/merge_requests/8815)
- Update redis to v7.2.11 (https://gitlab.com/gitlab-org/omnibus-gitlab/-/merge_requests/8821)
- [18.4] Upgrade Rack to 2.2.20 (https://gitlab.com/gitlab-org/omnibus-gitlab/-/merge_requests/8850)

18.3.6

- [18.3] Reduce cached SQL queries in `/api/v4/internal/pages` endpoint (https://gitlab.com/gitlab-org/gitlab/-/merge_requests/210366)
- [18.3] Update dependency openssl to v3.3.2 (https://gitlab.com/gitlab-org/gitlab/-/merge_requests/210403)
- [18.3] Update rexml to v3.4.4 (https://gitlab.com/gitlab-org/gitlab/-/merge_requests/210394)

- [18.3] Upgrade Rack to 2.2.20 (https://gitlab.com/gitlab-org/gitlab/-/merge_requests/210346)
- [18.3 Backport] Set http_continue_timeout to nil for s3 client (https://gitlab.com/gitlab-org/gitlab/-/merge_requests/211539)
- Backport of 'Fix redirect loop in Gitea rate limit' (https://gitlab.com/gitlab-org/gitlab/-/merge_requests/211473)
- Backport of Update Jira integration to use token-based pagination and Support Jira Cloud and Server issue fetching (https://gitlab.com/gitlab-org/gitlab/-/merge_requests/211572)
- [18.3] Uninstall rexml 3.4.0 and ensure 3.4.4 is used (https://gitlab.com/gitlab-org/omnibus-gitlab/-/merge_requests/8816)
- Update redis to v7.2.11 (https://gitlab.com/gitlab-org/omnibus-gitlab/-/merge_requests/8822)
- [18.3] Upgrade Rack to 2.2.20 (https://gitlab.com/gitlab-org/omnibus-gitlab/-/merge_requests/8851)

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 (https://docs.gitlab.com/ee/update/zero_downtime.html), this patch can be applied without downtime.

Post-deploy migrations

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

- 18.5.2
- 18.4.4

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

- Zero-downtime upgrades (https://docs.gitlab.com/ee/update/zero_downtime.html) for multi-node deployments
- Standard upgrades (https://docs.gitlab.com/update/package/#downtime) for single-node installations

Updating

To update GitLab, see the Update page (/update/). To update Gitlab Runner, see the Updating the Runner page (https://docs.gitlab.com/runner/install/linux-repository.html#updating-the-runner).

Receive Patch Notifications

To receive patch blog notifications delivered to your inbox, visit our contact us (https://about.gitlab.com/company/contact/) page. To receive release notifications via RSS, subscribe to our patch release RSS feed (https://about.gitlab.com/security-releases.xml) or our RSS feed for all releases (https://about.gitlab.com/all-releases.xml).

GitLab Patch Release: 18.5.2, 18.4.4, 18.3.6 via @gitlab

(http://twitter.com/share?
text=GitLab+Patch+Release%3A+18.5.2%2C+18.4.4%2C+18.3.6+via+%40gitlab&url=https://about.gitlab.com/rele
release-gitlab-18-5-2-released/&hashtags=)

Click to tweet!

security (/releases/categories/releases/#security)

(http://www.facebook.com/sharer.php?u=https://about.gitlab.com/releases/2025/11/12/patch-release-gitlab-18-5-2-released/) (http://www.linkedin.com/shareArticle?mini=true&url=https://about.gitlab.com/releases/2025/11/12/patch-release-gitlab-18-5-2-released/&title=GitLab Patch Release: 18.5.2, 18.4.4, 18.3.6) (https://news.ycombinator.com/submitlink?u=https://about.gitlab.com/releases/2025/11/12/patch-release-gitlab-18-5-2-released/&t=GitLab Patch Release: 18.5.2, 18.4.4, 18.3.6)

GitLab Patch Release: 18.5.1, 18.4.3, 18.3.5 (/releases/2025/10/22/patch-release-gitlab-18-5-1-released/)

GitLab 18.6 released with new UI designed for ... (/releases/2025/11/20/gitlab-18-6-released/)

Having trouble viewing or submitting this form?

We want to hear from you

Enjoyed reading this blog post or have questions or feedback? Share your thoughts by creating a new topic in the GitLab community forum.

Share your feedback

Take GitLab for a spin

See what your team could do with The DevSecOps Platform.

Get free trial (https://gitlab.com/-/trials/new?glm_content=default-saas-trial&glm_source=about.gitlab.com)

Have a question? We're here to help.

Talk to an expert.

®

Pricing

View plans (/pricing/)

Why Premium? (/pricing/premium/)

Why Ultimate? (/pricing/ultimate/)

Contact Us

Contact sales (/sales/)

Product

DevSecOps platform (/platform/)

AI-Assisted Development (/gitlab-duo/)

Topics

CICD (/topics/ci-cd/)