# GitLab Patch Release: 18.10.3, 18.9.5, 18.8.9

Today, we are releasing versions 18.10.3, 18.9.5, 18.8.9 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 |
|---|---|
| Exposed Method issue in websocket connections impacts GitLab CE/EE | High |
| Denial of Service issue in Terraform state lock API impacts GitLab CE/EE | High |
| Denial of Service issue in GraphQL API impacts GitLab CE/EE | High |
| Denial of Service issue in CSV import impacts GitLab CE/EE | Medium |
| Denial of Service issue in GraphQL SBOM API impacts GitLab EE | Medium |
| Code Injection issue in Code Quality reports impacts GitLab EE | Medium |
| Cross-site Scripting issue in analytics dashboards impacts GitLab EE | Medium |

| | |
|---|---|
| Improper Access Control issue in Environments API impacts GitLab EE | Medium |
| Information disclosure issue in CSV export impacts GitLab CE/EE | Medium |
| Missing Authorization issue in custom role permissions impacts GitLab CE/EE | Low |

## CVE-2026-5173 - Exposed Method issue in websocket connections impacts GitLab CE/EE

GitLab has remediated an issue that could have allowed an authenticated user to invoke unintended server-side methods through websocket connections due to improper access control.

**Impacted Versions:** GitLab CE/EE: all versions from 16.9.6 before 18.8.9, 18.9 before 18.9.5, and 18.10 before 18.10.3
**CVSS** 8.5 (`CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:L/A:N`)

This vulnerability has been discovered internally by GitLab team member Simon Tomlinson

## CVE-2026-1092 - Denial of Service issue in Terraform state lock API impacts GitLab CE/EE

GitLab has remediated an issue that could have allowed an unauthenticated user to cause denial of service due to improper input validation of JSON payloads.

**Impacted Versions:** GitLab CE/EE: all versions from 12.10 before 18.8.9, 18.9 before 18.9.5, and 18.10 before 18.10.3
**CVSS** 7.5 (`CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H`)

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

## CVE-2025-12664 - 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 denial of service by sending repeated GraphQL queries.

**Impacted Versions:** GitLab CE/EE: all versions from 13.0 before 18.8.9, 18.9 before 18.9.5, and 18.10 before 18.10.3
**CVSS** 7.5 (`CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H`)

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

## CVE-2026-1403 - Denial of Service issue in CSV import impacts GitLab CE/EE

GitLab has remediated an issue that when importing CSV files could have allowed an authenticated user to cause denial of service to Sidekiq workers due to improper validation of CSV file structure.

**Impacted Versions:** GitLab CE/EE: all versions from 11.7 before 18.8.9, 18.9 before 18.9.5, and 18.10 before 18.10.3
**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-2026-1101 - Denial of Service issue in GraphQL SBOM API impacts GitLab EE

GitLab has remediated an issue that could have allowed an authenticated user to cause denial of service to the GitLab instance

## CVE-2026-1516 - Code Injection issue in Code Quality reports impacts GitLab EE

GitLab has remediated an issue that in Code Quality reports could have allowed an authenticated user to leak IP addresses of users viewing the report via specially crafted content.

**Impacted Versions:** GitLab EE: all versions from 18.0.0 before 18.8.9, 18.9 before 18.9.5, and 18.10 before 18.10.3
**CVSS** 5.7 (`CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N`)

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

## CVE-2026-4332 - Cross-site Scripting issue in analytics dashboards impacts GitLab EE

GitLab has remediated an issue that, in customizable analytics dashboards, could have allowed an authenticated user to execute arbitrary JavaScript in the context of other users' browsers due to improper input sanitization.

**Impacted Versions:** GitLab EE: all versions from 18.2 before 18.8.9, 18.9 before 18.9.5, and 18.10 before 18.10.3
**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-2026-2619 - Incorrect Authorization issue in vulnerability flags AI detection API impacts GitLab EE

GitLab has remediated an issue that under certain circumstances could have allowed an authenticated user with auditor privileges to modify vulnerability flag data in private projects due to incorrect authorization.

**Impacted Versions:** GitLab EE: all versions from 18.6 before 18.8.9, 18.9 before 18.9.5, and 18.10 before 18.10.3
**CVSS** 4.3 (`CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N`)

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

## CVE-2025-9484 - Information Disclosure issue in certain GraphQl query impacts GitLab EE

GitLab has remediated an issue that under certain circumstances could have allowed an authenticated user to have access to other users' email addresses via certain GraphQL queries.

**Impacted Versions:** GitLab EE: all versions from 16.6 before 18.8.9, 18.9 before 18.9.5, and 18.10 before 18.10.3
**CVSS** 4.3 (`CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N`)

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

## CVE-2026-1752 - Improper Access Control issue in Environments API impacts GitLab EE

GitLab has remediated an issue that could have allowed an authenticated user with developer-role permissions to modify protected environment settings due to improper authorization checks in the API.

**Impacted Versions:** GitLab EE: all versions from 11.3 before 18.8.9, 18.9 before 18.9.5, and 18.10 before 18.10.3
**CVSS** 4.3 (`CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N`)

users via CSV export due to insufficient authorization checks.

**Impacted Versions:** GitLab CE/EE: all versions from 18.2 before 18.8.9, 18.9 before 18.9.5, and 18.10 before 18.10.3
**CVSS** 4.3 (`CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N`)

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

### CVE-2026-4916 - Missing Authorization issue in custom role permissions impacts GitLab CE/EE

GitLab has remediated an issue that could have allowed an authenticated user with custom role permissions to demote or remove higher-privileged group members due to improper authorization checks on member management operations.

**Impacted Versions:** GitLab CE/EE: all versions from 18.2 before 18.8.9, 18.9 before 18.9.5, and 18.10 before 18.10.3
**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

### 18.10.3

- [18.10] Revert “Merge branch ‘segregate-buildx-build-among-rails-ce-and-ee’ into ‘master’”
- chore: bump gitlab-zoekt to v1.11.1 on 18-10-stable
- Backport of Validate parallel:matrix expanded job name length
- Fix flaky spec in spec/requests/api/merge_requests_spec.rb
- Backport of Fix remaining failures in new_project_spec.rb after !228726
- Backport of ‘Fixes `gitlab-rspec` test failures on stable branches’
- Backport of ‘Upgrade http and llhttp-ffi’
- Backport ‘595107/fix-model-selection-ui-regression’ into 18.10
- [18.10] Remove me-south-1 region from AMI publishing list
- Backport 18.10: Do not include Spamcheck with the SLES12 package
- Backport 18-10: Set strategy:mirror to propagate downstream failure on check-packages-functionality trigger job

### 18.9.5

- [18.9] Fix composite identity support for dependency proxy access
- Fix flaky spec in spec/requests/api/merge_requests_spec.rb
- Backport of Fix remaining failures in new_project_spec.rb after !228726
- Backport ‘595107/fix-model-selection-ui-regression’ into 18.9
- [18.9] Remove me-south-1 region from AMI publishing list
- Backport 18.9: Do not include Spamcheck with the SLES12 package
- Backport 18-9: Set strategy:mirror to propagate downstream failure on check-packages-functionality trigger job

## Important notes on upgrading

These versions do not include any new migrations, and for multi-node deployments, should not require any downtime.

Please be aware that by default the Omnibus packages will stop, run migrations, and start again, no matter how "big" or "small" the upgrade is. This behavior can be changed by adding a `/etc/gitlab/skip-auto-reconfigure` file, which is only used for updates.

## Updating

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

Note: GitLab releases have skipped 18.10.2, 18.9.4 and 18.8.8. There are no patches with these version numbers.

## 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.