

Gitea 1.25.5 is released

March 16, 2026 · 9 min read



lunny

Gitea maintainer



1.25.5 Release

We're excited to announce the release of Gitea 1.25.5! We strongly recommend all users upgrade to this version, as it includes important security fixes, numerous bug fixes, and overall stability improvements.

- CVE-2026-25779: Prevent redirect bypasses via backslash-encoded paths ([#36660](#)) ([#36716](#)). Thanks to [@quirmz](#) for the report, and thanks to [@lunny](#) for the fix.
- CVE-2026-27660: Fix the release draft permission check ([#36659](#)) ([#36715](#)). Thanks to [@anticomputer](#) for the report, and thanks to [@lunny](#) for the fix.
- CVE-2026-27657: Fix an issue where a user could change another user's primary email address ([#36586](#)) ([#36607](#)). Thanks to [@CsEnox](#) for the report, and thanks to [@lunny](#) for the fix.
- CVE-2026-26232: Fix OAuth2 authorization code expiry and reuse handling ([#36797](#)) ([#36851](#)). Thanks to [@sammiee5311](#) for the report, and thanks to

[@lunny](#) for the fix.

- CVE-2026-22547: Add validation constraints for repository creation fields ([#36671](#)) ([#36757](#)). Thanks to [@brettm220](#) for the report, and thanks to [@lunny](#) for the fix.
- CVE-2026-24690: Fix permission checks for updating or rebasing pull request branches ([#36465](#)) ([#36838](#)). Thanks to the [CodeThreat Security Research Team](#) and [@Alexander Girgis](#) for the report, and thanks to [@lunny](#) for the fix.
- CVE-2026-26292: Add HTTP transport support for LFS in push/sync mirror migrations ([#36665](#)) ([#36691](#)). Thanks to [@allsmog](#) for the report, and thanks to [@lunny](#) for the fix.
- CVE-2026-20909: Fix the track time list permission check ([#36662](#)) ([#36744](#)).
- CVE-2026-25782: Fix incorrect issue ID handling in time tracking ([#36664](#)) ([#36689](#)). Thanks to [@CsEnox](#) for the report, and thanks to [@lunny](#) for the fix.
- CVE-2026-25718: Fix path resolution handling ([#36734](#)) ([#36746](#)). Thanks to [@yonatan-pl](#) for the report, and thanks to [@wxiaoguang](#) for the fix.
- CVE-2026-28705: Fix a bug affecting release asset dumping ([#36799](#)) ([#36839](#)). Thanks to Robert Flosbach from Neodyme AG for the report, and thanks to [@lunny](#) for the fix.
- CVE-2026-25712: Fix org permission API visibility checks for hidden members and private organizations ([#36798](#)) ([#36841](#)). Thanks to Maximilian Luff (<https://github.com/maluff>), Daniel Zahl (<https://github.com/Sai2r>), Marcus Gelderie (<https://github.com/mgelde>) for the report, and thanks to [@lunny](#) for the fix.
- CVE-2026-27779: Fix forwarded proto handling for public URL detection ([#36810](#)) ([#36836](#)). Thanks to fed01k for the report and thanks to [@lunny](#) for the fix.
- CVE-2026-26307: Add a timeout for `git grep` searches ([#36809](#)) ([#36835](#)). Thanks to uug4na for the report, and thanks to [@lunny](#) for the fix.
- CVE-2026-26247: Fix OAuth2 S256 handling ([#36462](#)) ([#36477](#)). Thanks to Aisle Research for the report, and thanks to [@lunny](#) for the fix.

Dependency Update

Go upgrades to 1.25.8 which includes security fixes

This release includes [42 merged pull requests](#), thanks to the amazing contributions from our community.

How to install or update

Download our pre-built binaries from the [Gitea downloads page](#) - make sure to select the version compatible with your platform. For a step-by-step guide on installation or upgrades, check out our [installation documentation](#)

Special Thanks

We would also like to thank all of our supporters on [Open Collective](#) who are helping to sustain us financially.

Looking for a seamless, hassle-free solution to manage your Git repositories? Discover [Gitea Cloud](#) - A fully-managed, scalable platform designed to streamline your development workflow.

Changelog

- SECURITY
 - Toolchain Update to Go 1.25.6 ([#36480](#)) ([#36487](#))
 - Adjust the toolchain version ([#36537](#)) ([#36542](#))
 - Update toolchain to 1.25.8 for v1.25 ([#36888](#))
 - Prevent redirect bypasses via backslash-encoded paths ([#36660](#)) ([#36716](#))
 - Fix get release draft permission check ([#36659](#)) ([#36715](#))
 - Fix a bug user could change another user's primary email ([#36586](#)) ([#36607](#))
 - Fix OAuth2 authorization code expiry and reuse handling ([#36797](#)) ([#36851](#))
 - Add validation constraints for repository creation fields ([#36671](#)) ([#36757](#))
 - Fix bug to check whether user can update pull request branch or rebase branch ([#36465](#)) ([#36838](#))
 - Add migration http transport for push/sync mirror lfs ([#36665](#)) ([#36691](#))
 - Fix track time list permission check ([#36662](#)) ([#36744](#))
 - Fix track time issue id ([#36664](#)) ([#36689](#))

- Fix path resolving ([#36734](#)) ([#36746](#))
- Fix dump release asset bug ([#36799](#)) ([#36839](#))
- Fix org permission API visibility checks for hidden members and private orgs ([#36798](#)) ([#36841](#))
- Fix forwarded proto handling for public URL detection ([#36810](#)) ([#36836](#))
- Add a git grep search timeout ([#36809](#)) ([#36835](#))
- Fix oauth2 s256 ([#36462](#)) ([#36477](#))
- ENHANCEMENTS
 - Make `security-check` informational only ([#36681](#)) ([#36852](#))
 - Upgrade to github.com/cloudflare/circl 1.6.3, svgo 4.0.1, markdownlint-cli 0.48.0 ([#36840](#))
 - Add some validation on values provided to USER_DISABLED_FEATURES and EXTERNAL_USER_DISABLED_FEATURES ([#36688](#)) ([#36692](#))
 - Upgrade gogit to 5.16.5 ([#36687](#))
 - Add wrap to runner label list ([#36565](#)) ([#36574](#))
 - Add dnf5 command for Fedora in RPM package instructions ([#36527](#)) ([#36572](#))
 - Allow scroll propagation outside code editor ([#36502](#)) ([#36510](#))
- BUGFIXES
 - Fix non-admins unable to automerge PRs from forks ([#36833](#)) ([#36843](#))
 - Fix bug when pushing mirror with wiki ([#36795](#)) ([#36807](#))
 - Fix artifacts v4 backend upload problems ([#36805](#)) ([#36834](#))
 - Fix CRAN package version validation to allow more than 4 version components ([#36813](#)) ([#36821](#))
 - Fix force push time-line commit comments of pull request ([#36653](#)) ([#36717](#))
 - Fix SVG height calculation in diff viewer ([#36748](#)) ([#36750](#))
 - Fix push time bug ([#36693](#)) ([#36713](#))
 - Fix bug the protected branch rule name is conflicted with renamed branch name ([#36650](#)) ([#36661](#))
 - Fix bug when do LFS GC ([#36500](#)) ([#36608](#))
 - Fix focus lost bugs in the Monaco editor ([#36609](#))
 - Reprocess htmx content after loading more files ([#36568](#)) ([#36577](#))

- Fix assignee sidebar links and empty placeholder ([#36559](#)) ([#36563](#))
- Fix issues filter dropdown showing empty label scope section ([#36535](#)) ([#36544](#))
- Fix various mermaid bugs ([#36547](#)) ([#36552](#))
- Fix data race when uploading container blobs concurrently ([#36524](#)) ([#36526](#))
- Correct spacing between username and bot label ([#36473](#)) ([#36484](#))

Contributors

- [@ChristopherHX](#)
- [@copilot](#)
- [@lunny](#)
- [@noeljackson](#)
- [@POPSuL](#)
- [@sebastianertz](#)
- [@silverwind](#)
- [@tyroneye](#)
- [@wxiaoguang](#)
- [@yshyuk](#)
- [@Zetta123](#)
- [@ZPascal](#)

Tags: [release](#)



Join our community

Gitea is open source. Star our GitHub repo, and join our community on Discord!

[GO TO GITHUB >](#) [JOIN DISCORD >](#)



Subscribe to our newsletter

Stay up to date with all things Gitea

Subscribe