Gitea 1.26.3 and 1.26.4 are released

June 21, 2026 · 8 min read

bircni
Gitea maintainer

We are excited to announce the release of **Gitea 1.26.3** and **Gitea 1.26.4**. Version 1.26.3 delivers a large set of security fixes alongside important bug fixes and stability improvements. Version 1.26.4 follows immediately with a fix for a repository code-page regression introduced in 1.26.3 and an additional security fix.

We strongly recommend upgrading directly to 1.26.4. If you are already on 1.26.3, please upgrade to 1.26.4 as soon as possible.

1.26.4

This release fixes the **"context deadline exceeded"** regression from 1.26.3, where repository code pages could fail to load (#38177). `WalkGitLog` now handles EOF and context errors correctly (#38185). Thanks to @wxiaoguang for the fix.

It also addresses the following security advisory:

- Do not auto-reactivate disabled users on the OAuth2 sign-in callback (#38183). Thanks to @chndlrx for the report, and @bircni for the fix.

This release includes 2 merged pull requests in the milestone.

Special thanks to @wxiaoguang for the quick hotfix.

1.26.3

This release addresses a number of security advisories. Several of them bundle multiple fixes into combined pull requests (#38151 and #38147).

- CVE-2026-20896: The Docker images shipped a `REVERSE_PROXY_TRUSTED_PROXIES = *` default, which let any source IP impersonate any user via the `X-WEBAUTH-USER` header. Reverse-proxy authentication is now opt-in and admin-configured (#38151). Thanks to Joshua Martinelle with Tenable / bughunters@tenable and @rz1027 for the report, and @bircni for the fix.
- CVE-2026-22874: Tighten the default allow-list filter used by webhooks and migrations to close an incomplete SSRF protection that could reach internal addresses (#38173, #38059). Thanks to @JLLeitschuh for the report, and @TheFox0x7 and @bircni for the fix.
- CVE-2026-27775: Re-check branch write permission for every ref in a push; the pre-receive hook cached the first ref's result, letting a per-branch maintainer-edit grant escalate to full repository write (#38151). Thanks to @adrian-doyensec for the report, and @bircni for the fix.
- CVE-2026-24451: Block fork synchronization (`merge-upstream`) when the base repository is no longer readable, so a fork can no longer pull commits made after its parent was switched from public to private (#38151). Thanks to @ybsun0215 for the report, and @bircni for the fix.
- CVE-2026-20779: Enforce single-use TOTP passcodes across web login, password reset, and the Basic-Auth `X-Gitea-OTP` surface, closing a TOCTOU race and a

stateless replay window (#38151). Thanks to @Kript0r3x for the report, and @bircni for the fix.

- CVE-2026-28740: Require Code-unit access for cross-repository LFS object reuse, so a non-Code grant can no longer authorize private source objects (#38050). Thanks to @m2hcz for the report, and @bircni for the fix.
- Reject unknown SSH LFS sub-verbs to close an authentication bypass that allowed unauthorized read access to private repositories (#38015). Thanks to @Tomer-PL for the report, and @bircni for the fix.
- Require a fork pull request to be merged before it can bypass the workflow approval gate, fixing a permanent approval-gate bypass (#38041). Thanks to @prakhar0x01 for the report, and @bircni for the fix. See the breaking-change note below.
- CVE-2026-27761: Enforce repository token scope on the RSS/Atom feed endpoints, so a personal access token without repository scope can no longer read private repository commit data (#38147). Thanks to @babakizo420 for the report, and @bircni for the fix.
- CVE-2026-25038: Enforce organization visibility on the organization label read endpoints so private organization labels no longer leak to non-members (#38151). Thanks to @ybsun0215 for the report, and @bircni for the fix.
- Block HTTP redirects during repository migration clones to prevent SSRF reaching internal addresses through an attacker-controlled redirect (#38147). Thanks to @moltenbit for the report, and @bircni for the fix.
- Bound CODEOWNERS pattern matching time to prevent an unauthenticated ReDoS denial of service (#38025). Thanks to @AdamKorcz for the report, and @bircni for the fix.
- Redact the notification subject after repository access is revoked, so private issue and pull request metadata is no longer leaked through the notification API (#38147). Thanks to @ybsun0215 for the report, and @bircni for the fix.

This release also includes additional security hardening that bounds Debian control-file parsing to a single stanza (#38055) and updates `golang.org/x/net` to v0.55.0 (#37829).

This release includes 31 merged pull requests, thanks to the amazing contributions from our community.

Breaking change

This release tightens the fork pull request approval gate: a pull request from a fork must now be merged before it can bypass the approval gate (#38041). Review your workflow approval settings if you rely on the previous behavior.

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.

Changelog

1.26.4 - 2026-06-21

- SECURITY
  - Do not auto-reactivate disabled users on OAuth2 callback (#38183)
- BUGFIXES
  - Fix `WalkGitLog` context error handling so repository code pages load correctly (#38185)

1.26.3 - 2026-06-20

- BREAKING
  - Require merged PR to bypass fork PR approval gate (#38041)
- SECURITY
  - Patch incorrect host matcher private list (#38173)
  - Various security fixes (#38151)
  - Various security fixes (#38147)
  - Allow git clone of private repos with anonymous code access (#38146)
  - Ignore stale OIDC external login links to organizations (#38141)
  - Block reserved IP ranges from external/private host matcher filters (#38059)
  - Require Code-unit access for cross-repo LFS object reuse (#38050)
  - Reject unknown SSH LFS sub-verbs to prevent auth bypass (#38015)
  - Bound CODEOWNERS regex match time (#38025)
  - Bound Debian `ParseControlFile` to a single control stanza (#38055)
  - Update module golang.org/x/net to v0.55.0 [security] (#37829)
- API
  - Add Link header in `ListForks` (#38063)
- BUGFIXES
  - Fix the panic when ssh remote LFS endpoint parsing fails (#38158)
  - Fix nil pointer panic when filtering tracked times by a non-existent user (#38115)
  - Keep literal "false" value displayed in `workflow_dispatch` choice dropdowns (#38096)
  - Parse HEAD ref (#38119)
  - Fix git cmd (#38087)
  - Generate release notes for initial tag (#37986)
  - Return 404 when job log blob is missing (#38004)
  - Exclude `workflow_call` from workflow trigger detection (#37899)

  - Keep action run title clickable when commit subject is a URL (#37898)
  - Reject `workflow_dispatch` for workflows without that trigger (#37895)
  - Ack re-sent `UpdateLog` finalize idempotently (#37892)
  - Fix http content file render (#37856)
  - Clear stale `ReviewTypeRequest` when submitting pending review (#37815)
  - Fix issue target branch selection for non-collaborators (#38164)
- BUILD
  - Update `@playwright/test` to 1.60.0 (#38144)
  - Add `tools/ci-tools.ts` for the PR labeler workflow (#37831)
  - Fix swagger css import (#37803)

Tags: release