GitLab Patch Release: 19.1.1, 19.0.3, 18.11.6

On June 24, 2026, we released versions 19.1.1, 19.0.3, 18.11.6 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 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
Cross-site Scripting issue in Analytics Dashboard impacts GitLab EE	High
Cross-site Scripting issue in Web IDE workbench asset handler impacts GitLab CE/EE	High
Information Disclosure issue in Duo Workflows impacts GitLab EE	High
Authorization Bypass issue in Virtual Registry Cleanup Policy API impacts GitLab EE	Medium
Improper Authorization issue in Rapid Diffs impacts GitLab CE/EE	Medium
Incorrect Authorization issue in DAST scanner and site profile management impacts GitLab EE	Medium
Insufficient Filtering issue in CI/CD API impacts GitLab CE/EE	Medium
Improper Input Validation issue in Snippets impacts GitLab CE/EE	Medium
Incorrect Authorization issue in Maven Package Registry impacts GitLab CE/EE	Medium

Improper Access Control issue in group packages API impacts GitLab CE/EE	Medium
Improper Access Control issue in Protected Environments API impacts GitLab EE	Low
Missing Authorization issue in Security Dashboard impacts GitLab EE	Low
Server-Side Request Forgery issue in Repository Mirroring impacts GitLab CE/EE	Low

CVE-2026-10086 - Cross-site Scripting issue in Analytics Dashboard impacts GitLab EE

GitLab has remediated an issue that under certain conditions could have allowed an authenticated user with developer-role permissions to execute arbitrary client-side code in the context of another user's session, due to improper sanitization of user-supplied input.

Impacted Versions: GitLab EE: all versions from 16.4 before 18.11.6, 19.0 before 19.0.3, and 19.1 before 19.1.1
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-2026-10712 - Cross-site Scripting issue in Web IDE workbench asset handler impacts GitLab CE/EE

GitLab has remediated an issue that could have allowed an unauthenticated user to execute arbitrary JavaScript in a user's browser session due to improper path validation under certain conditions.

Impacted Versions: GitLab CE/EE: all versions from 18.10 before 18.11.6, 19.0 before 19.0.3, and 19.1 before 19.1.1
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-2026-12053 - Information Disclosure issue in Duo Workflows impacts GitLab EE

GitLab has remediated an issue that under certain conditions could have allowed a user to access sensitive information that had already been committed to a project, due to insufficient output filtering in Duo Workflows.

Impacted Versions: GitLab EE: all versions from 19.1 before 19.1.1
CVSS 7.7 (`CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N`)

Thanks 3nvz and GitLab team member Dennis Appelt for reporting this vulnerability

CVE-2026-5309 - Authorization Bypass issue in Virtual Registry Cleanup Policy API impacts GitLab EE

GitLab has remediated an issue that under certain conditions could have allowed an authenticated user to read or modify another group's virtual registry cleanup policy settings without authorization.

Impacted Versions: GitLab EE: all versions from 18.6 before 18.11.6, 19.0 before 19.0.3, and 19.1 before 19.1.1
CVSS 5.4 (`CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N`)

Thanks go7f0 for reporting this vulnerability through our HackerOne bug bounty program

GitLab Docs

issue references on public projects due to improper authorization checks.

Impacted Versions: GitLab CE/EE: all versions from 17.5 before 18.11.6, 19.0 before 19.0.3, and 19.1 before 19.1.1
CVSS 5.3 (`CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N`)

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

CVE-2026-11379 - Incorrect Authorization issue in DAST scanner and site profile management impacts GitLab EE

GitLab has remediated an issue in GitLab EE affecting all versions from 13.11 prior to 18.11.6, 19.0 prior to 19.0.3, and 19.1 prior to 19.1.1 in which incorrect authorization in DAST site profile management could allow a user with Developer role to exfiltrate DAST site profile secrets under certain conditions.

Impacted Versions: GitLab EE: all versions from 13.11 before 18.11.6, 19.0 before 19.0.3, and 19.1 before 19.1.1
CVSS 5.3 (`CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N`)

This vulnerability has been discovered internally by GitLab team member David Nelson

CVE-2026-8330 - Insufficient Filtering issue in CI/CD API impacts GitLab CE/EE

GitLab has remediated an issue that under certain conditions could have allowed sensitive information to be written to application logs due to insufficient filtering in a CI/CD API endpoint.

Impacted Versions: GitLab CE/EE: all versions from 9.3 before 18.11.6, 19.0 before 19.0.3, and 19.1 before 19.1.1
CVSS 4.4 (`CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N`)

This vulnerability has been discovered internally by GitLab team member Joel Clarke

CVE-2026-1606 - Improper Input Validation issue in Snippets impacts GitLab CE/EE

GitLab has remediated an issue that under certain conditions could have allowed an authenticated user to conceal content within a Snippet due to improper input validation.

Impacted Versions: GitLab CE/EE: all versions from 14.8 before 18.11.6, 19.0 before 19.0.3, and 19.1 before 19.1.1
CVSS 4.3 (`CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N`)

Thanks st4nly0n for reporting this vulnerability through our HackerOne bug bounty program

CVE-2026-5952 - Incorrect Authorization issue in Maven Package Registry impacts GitLab CE/EE

GitLab has remediated an issue that under certain conditions could have allowed an authenticated user with developer-role permissions to bypass package protection rules and overwrite protected Maven package metadata due to incorrect authorization checks.

Impacted Versions: GitLab CE/EE: all versions from 17.11 before 18.11.6, 19.0 before 19.0.3, and 19.1 before 19.1.1
CVSS 4.3 (`CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N`)

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

GitLab has remediated an issue that under certain conditions could have allowed an authenticated user with Reporter-level group permissions to view package metadata from projects with the Package Registry disabled due to incorrect authorization checks in the group packages feature.

Impacted Versions: GitLab CE/EE: all versions from 13.6 before 18.11.6, 19.0 before 19.0.3, and 19.1 before 19.1.1
CVSS 4.3 (`CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N`)

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

CVE-2026-0934 - Improper Access Control issue in Protected Environments API impacts GitLab EE

GitLab has remediated an issue that under certain conditions could have allowed an authenticated user with custom role permissions to view, create, or delete protected environment configurations despite CI/CD visibility being disabled for the project.

Impacted Versions: GitLab EE: all versions from 17.9 before 18.11.6, 19.0 before 19.0.3, and 19.1 before 19.1.1
CVSS 3.8 (`CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:N`)

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

CVE-2026-3176 - Missing Authorization issue in Security Dashboard impacts GitLab EE

GitLab has remediated an issue that under certain conditions could have allowed an authenticated user with limited permissions to access project information due to insufficient authorization checks.

Impacted Versions: GitLab EE: all versions from 18.6 before 18.11.6, 19.0 before 19.0.3, and 19.1 before 19.1.1
CVSS 3.1 (`CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N`)

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

CVE-2026-12635 - Server-Side Request Forgery issue in Repository Mirroring impacts GitLab CE/EE

GitLab has remediated an issue that under certain conditions could have allowed an authenticated user with maintainer-role permissions to make requests to internal network resources through mirror synchronization due to improper URL validation.

Impacted Versions: GitLab CE/EE: all versions from 8.3 before 18.11.6, 19.0 before 19.0.3, and 19.1 before 19.1.1
CVSS 3.1 (`CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N`)

This vulnerability has been discovered internally by GitLab team member Félix Veillette-Potvin

Bug fixes

19.1.1

- Backport final 19.1 release notes
- Backport fix flaky N+1 REST API spec
- [19.1] Backport of Revert “Merge branch ‘587231-update-session-list-item-format’ into ‘master’”
- Backport of “Remove GIT_CONFIG_GLOBAL=/dev/null from Duo Workflow git hardening”
- Backport of ‘Fix wrong argument’
- Exclude .agents and .claude dirs from gitlab-rails package
- [19.1] Normalize falsey smtp_authentication to disable SMTP auth

GitLab Docs

19.0.3

- Update yq to 4.53.3 - Backport to 19-0
- 19-0 Backport: Update azcopy to version 10.32.4
- 19-0 Backport: Update PyOpenSSL to 25.3.0 and pin python-cryptography to 46.0.7
- Backport of ‘Filter group template projects by user visibility and membership’
- Backport of “Treat split failure reasons as retry:when aliases”
- Backport of ‘Allow URL import into groups when personal project creation disabled’ to 19.0
- 19.0 Backport of ‘Add index on security_findings for keyset pagination’
- Backport of ‘Fix Amazon Q usage quota check’ into 19.0
- Backport of ‘Fix 500 on multi-arch tags on the legacy registry path’ into 19.0
- Backport ‘Restore admin-level user data read access for auditors in Users API’ to 19.0
- Backport: Fix UUID calibration with multiple branch tracking
- Backport of ‘Fix: Embeddings Indexing: `nil` user error in embeddings client’
- [19.0] Backport of Revert “Merge branch ‘587231-update-session-list-item-format’ into ‘master’”
- Backport of “fix: Fix malformed safe.directory in workflows”
- Backport of ‘Fix award emoji and note updates not reflecting live on MR page’ to 19.0
- Bump ERB gem to 4.0.3.1
- Default registry database port to postgresql[‘port’] (19.0 backport)
- Exclude .agents and .claude dirs from gitlab-rails package
- [19.0] Normalize falsey smtp_authentication to disable SMTP auth
- Backport SLES 15.6 extended support into 19-0-stable

18.11.6

- Update yq to 4.53.3 - Backport to 18-11
- 18-11 Backport: Update azcopy to 10.32.4
- 18-11 Backport: Update PyOpenSSL to 25.3.0 and pin python-cryptography to 46.0.7
- Temporarily allow issue-bot to fail (backport to 18-11-stable)
- Backport of ‘Allow job token basic auth for generic package upload’ to 18.11
- Backport “Bump devfile gem to 0.5.2” to 18-11-stable-ee
- Backport of ‘Fix SM direct access spec to expect 403’ into 18.11
- 18.11 Backport of ‘Add index on security_findings for keyset pagination’
- Backport of ‘Fix Amazon Q usage quota check’ into 18.11
- Backport of ‘Fix 500 on multi-arch tags on the legacy registry path’ into 18.11
- [18.11] Backport of Revert “Merge branch ‘587231-update-session-list-item-format’ into ‘master’”
- Backport of “fix: Fix malformed safe.directory in workflows”
- Backport of ‘Fix award emoji and note updates not reflecting live on MR page’ to 18.11
- Bump ERB gem to 4.0.3.1
- Default registry database port to postgresql[‘port’] (18.11 backport)

Important notes on upgrading

This patch includes database migrations that may impact your upgrade process.

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:

- 19.0.3
- 18.11.6

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

Updating

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