GitLab Critical Security Release: 16.8.1, 16.7.4, 16.6.6, 16.5.8

On January 25, 2024, we released versions 16.8.1, 16.7.4, 16.6.6, 16.5.8 for GitLab Community Edition (CE) and Enterprise Edition (EE).

These versions contain important security fixes, and we strongly recommend that all GitLab installations be upgraded to one of these versions immediately. GitLab.com and GitLab Dedicated environments are already running the patched version.

GitLab releases patches for vulnerabilities in dedicated security releases. There are two types of security releases: a monthly, scheduled security release, released a week after the feature release (which deploys on the 3rd Thursday of each month), and ad-hoc security releases for critical vulnerabilities. For more information, you can visit our security FAQ. You can see all of our regular and security release blog posts here. In addition, the issues detailing each vulnerability are made public on our issue tracker 30 days after the release in which they were patched.

We are dedicated to ensuring all aspects of GitLab that are exposed to customers or that host customer data are held to the highest security standards. As part of maintaining good security hygiene, it is highly recommended that all customers upgrade to the latest security 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, this means all types are affected.

Table of fixes

Title	Severity
Arbitrary file write while creating workspace	Critical
ReDoS in `Cargo.toml` blob viewer	Medium
Arbitrary API PUT requests via HTML injection in user's name	Medium
Disclosure of the public email in Tags RSS Feed	Medium
Non-Member can update MR Assignees of owned MRs	Medium

Arbitrary file write while creating workspace

An issue has been discovered in GitLab CE/EE affecting all versions from 16.0 prior to 16.5.8, 16.6 prior to 16.6.6, 16.7 prior to 16.7.4, and 16.8 prior to 16.8.1 which allows an authenticated user to write files to arbitrary locations on the GitLab server while creating a workspace. This is a critical severity issue (`CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H`, 9.9). It is now mitigated in the latest release and is assigned CVE-2024-0402.

The fix for this security vulnerability has been backported to 16.5.8 in addition to 16.6.6, 16.7.4, and 16.8.1. GitLab 16.5.8 *only* includes a fix for this vulnerability and does *not* contain any of the other fixes or changes mentioned in this blog post.

ReDoS in `Cargo.toml` blob viewer

An issue has been discovered in GitLab CE/EE affecting all versions from 12.7 prior to 16.6.6, 16.7 prior to 16.7.4, and 16.8 prior to 16.8.1 It was possible for an attacker to trigger a Regular Expression Denial of Service via a `Cargo.toml` containing maliciously crafted input. This is a medium severity issue (`CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H`, 6.5). It is now mitigated in the latest release and is assigned CVE-2023-6159.

Thanks yvvdwf for reporting this vulnerability through our HackerOne bug bounty program.

Arbitrary API PUT requests via HTML injection in user's name

An issue has been discovered in GitLab CE/EE affecting all versions after 13.7 before 16.6.6, 16.7 prior to 16.7.4, and 16.8 prior to 16.8.1. Improper input sanitization of user name allows arbitrary API PUT requests. This is a medium severity issue (`CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:N`, 6.4). It is now mitigated in the latest release and is assigned CVE-2023-5933.

Thanks yvvdwf for reporting this vulnerability through our HackerOne bug bounty program.

Disclosure of the public email in Tags RSS Feed

An issue has been discovered in GitLab affecting all versions before 16.6.6, 16.7 prior to 16.7.4, and 16.8 prior to 16.8.1. It was possible to read the user email address via tags feed although the visibility in the user profile has been disabled. This is a medium severity issue (`CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N`, 5.3). It is now mitigated in the latest release and is assigned CVE-2023-5612.

Thanks erruqill for reporting this vulnerability through our HackerOne bug bounty program.

Non-Member can update MR Assignees of owned MRs

An authorization vulnerability exists in GitLab versions 14.0 prior to 16.6.6, 16.7 prior to 16.7.4, and 16.8 prior to 16.8.1. An unauthorized attacker is able to assign arbitrary users to MRs that they created within the project . This is a medium severity issue (`CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N`, 4.3). It is now mitigated in the latest release and is assigned CVE-2024-0456.

Thanks to Niklas for reporting this vulnerability.

Update xmlsoft/libxml2 to >= v2.11.6

The `xmlsoft/libxml2` version has been upgraded to 2.12.3 to mitigate CVE-2023-45322.

Upgrade redis to address CVE-2023-41056 (Redis RCE)

Redis has been upgraded to version 7.0.15 to mitigate CVE-2023-41056.

Non Security Patches

16.8.1

- Update dependency gitlab-glfm-markdown to '~> 0.0.11'
- Backport Redis migration to 16.8
- [Backport] Optimize garbage collection process
- [Backport] Bump GitLab Shell version to 14.33.0

- Sync chef-gem and chef-bin (16.7)

16.6.6

- Backport: Move release-environments pipeline to be sourced from master
- Backport - Bring legacy verification behavior back for repositories

Updating

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

Receive Security Release Notifications

To receive security release blog notifications delivered to your inbox, visit our contact us page. To receive release notifications via RSS, subscribe to our security release RSS feed or our RSS feed for all releases.