January 25, 2024

Overall rating: Critical

This notification is intended as an informational bulletin for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware that GitLab published a security advisory to address critical vulnerabilities in the following products:

- GitLab Community Edition (CE) – multiple versions
- GitLab Enterprise Edition (EE) – multiple versions

Technical Details

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.

These vulnerabilities are rated as an overall **Critical** Severity.

Recommended Action

- Investigate how your area of responsibility is affected.
- Notify business owner(s) as required.
- *Ensure mitigation is performed at your next change window.*

Please notify VRM with any questions or concerns you may have.

References

- CVE-2024-0402, CVE-2023-6159, CVE-2023-5933, CVE-2023-5612, CVE-2024-0456
- GitLab Security Advisory
- GitLab Releases