# Last commit message, description & sha1 hash of a private repo in a private group is leaked to guest users through merge request

HackerOne report #1465994 by albatraoz on 2022-01-31, assigned to GitLab Team:

Report | Attachments | How To Reproduce

## Report

### Summary

Commit related details like commit message, description, sha1, etc are leaked to demoted guest users who should not have access to the repository of a private project according to the <u>permission model</u>. This information is leaked through a fork of the project created by the user(reporter/developer) before being demoted to guest. Once being demoted to guest, the user is able to sneak all the latest commits to the parent branch.

#### Steps to reproduce

- 1. Create a private project in a group as user A.
- 2. Add User B as a reporter to this project.
- 3. As User B create a fork of the project on you personal namespace.
- 4. As User A demote User B to guest from the group settings.
- 5. As User B visit the forked repo & go to the create new merge request. In the target branch you will see the parent branch is selected & the commit message is being leaked.
- 6. As User A add a new commit message to the parent branch.
- 7. As User B refresh the page opened in step 5 & you will see the latest commit added by User A in step 6.

#### POC

Attaching a video as POC for easier reproduction of the issue

0:00 / 2:20

## commit leak.mp4

## **Impact**

An attacker would be able to snoop into commit messages on the default branch even after being demoted to guest user. These commit messages or descriptions may include confidential information to the repo like unreleased features/ vulnerability information, etc

## **Attachments**

Warning: Attachments received through HackerOne, please exercise caution!

• commit leak.mp4

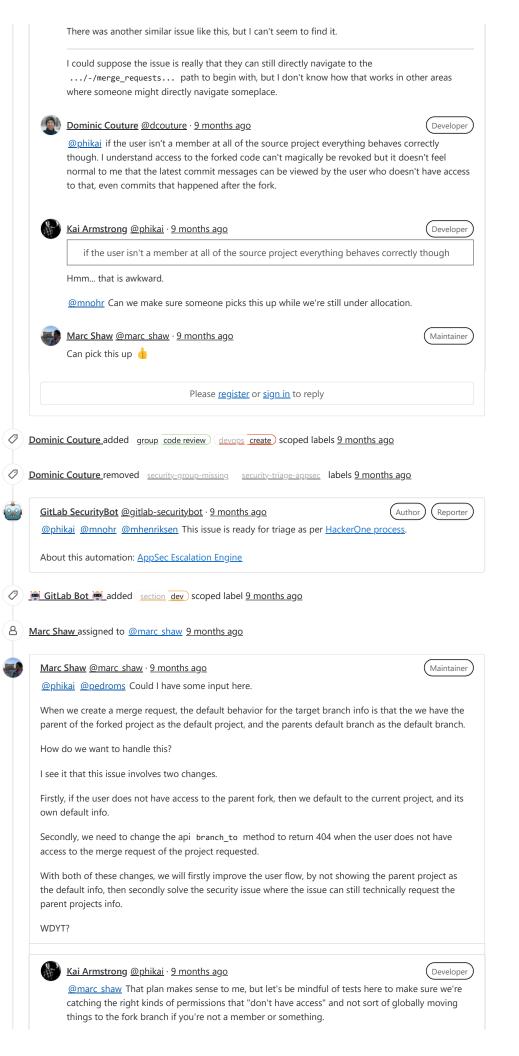
# **How To Reproduce**

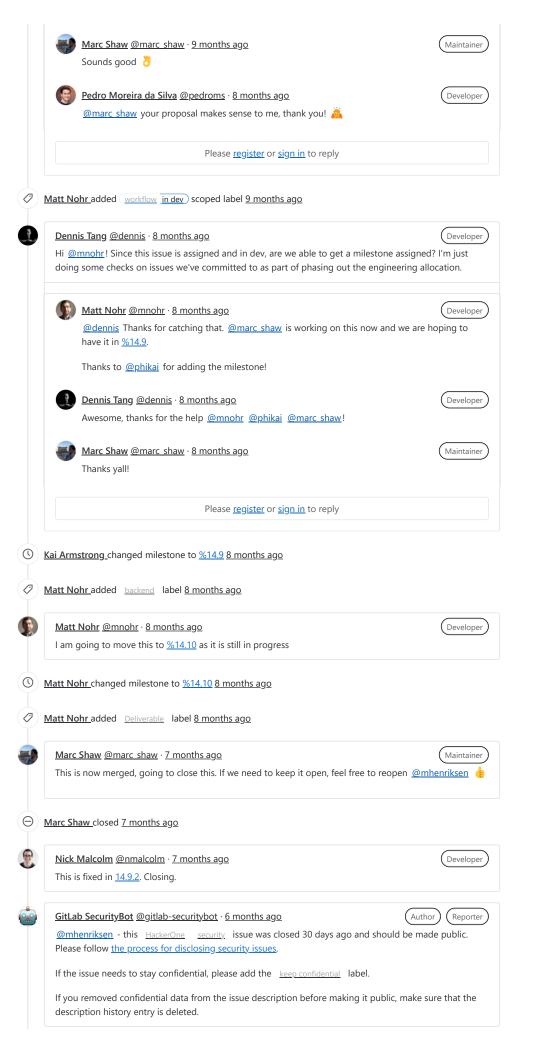
Please add  $\underline{\text{reproducibility information}}$  to this section:

- 1.
- 2.
- 3.

 ⚠ Drag your designs here or <u>click to upload</u>.

No tasks are currently assigned. Use tasks to break down this issue into smaller parts. Linked items □ 0 Link issues together to show that they're related or that one is blocking others. Learn more. Activity GitLab SecurityBot changed due date to April 26, 2022 9 months ago GitLab SecurityBot added Weakness CWE-284 bug vulnerability type bug priority 3 severity 3 scoped labels 9 months ago GitLab SecurityBot added HackerOne security labels 9 months ago GitLab SecurityBot @gitlab-securitybot · 9 months ago ( Author Reporter HackerOne comment by forest\_dweller: Hi [@]albatraoz, Thank you for your submission. I hope you are well. Your report is currently being reviewed and the HackerOne triage team will get back to you once there is additional information to share. Have a great day! Kind regards, [@]forest\_dweller GitLab SecurityBot @gitlab-securitybot · 9 months ago Author ( Reporter HackerOne comment by forest\_dweller: Hi [@]albatraoz, Thank you for your report! I'm discussing this submission internally with the GitLab team. You will be updated as soon as there is additional information to share. Thank you for your patience! Cheers, [@]forest\_dweller <u>GitLab SecurityBot</u> @gitlab-securitybot · 9 months ago (Author Reporter **<u>HackerOne comment</u>** by dcouture: Setting attack complexity to high given the preconditions (be a member of a project, fork and then be demoted) that needs to happen to make this vulnerability exploitable (2) GitLab SecurityBot added security-group-missing security-triage-appsec labels 9 months ago Dominic Couture @dcouture · 9 months ago Hello <a href="mailto:mphikai">mphikai</a> <a href="mailto:mphikai">mmnohr</a> <a href="mailto:mphikai">mnohr</a> <a href see code-related information) can see the latest commit messages by attempting to open an MR from a fork they have created before being demoted. Elaborate setup but still something that shouldn't happen. https://gitlab.com/<group>/<project>/-/merge\_requests/new/branch\_to?target\_project\_id= <id>&ref=<refname> is the URL leaking the information. Kai Armstrong @phikai · 9 months ago Developer @dcouture I don't think we've considered fork items like this to be security issues. As soon as you allow forks to be created there's nothing we can really do about this because we can't break the relationships. There's a security control available in premium for this: https://docs.gitlab.com/ee/user/group/#prevent-project-forking-outside-group which restricts access to forking outside of the group so that these kinds of things can't happen.





( <u>Michael Henriksen</u> made the issue visible to everyone <u>6 months ago</u>

Please <u>register</u> or <u>sign in</u> to reply