

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 [permission model](#). 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 [reproducibility information](#) to this section:

- 1.
- 2.
- 3.

 Drag your designs here or [click to upload](#).

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 [@]albatraz,

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 [@]albatraz,

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



GitLab SecurityBot @gitlab-securitybot · 9 months ago

Author

Reporter

[HackerOne comment](#) 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



GitLab SecurityBot added [security-group-missing](#) [security-triage-appsec](#) labels 9 months ago



Dominic Couture @dcouture · 9 months ago

Developer

Hello @phikai @mnohr 🙌 Private project members who have been demoted to guest (and shouldn't 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.

There was another similar issue like this, but I can't seem to find it.

I could suppose the issue is really that they can still directly navigate to the
.../-/merge_requests... path to begin with, but I don't know how that works in other areas
where someone might directly navigate someplace.



Dominic Couture @dcouture · 9 months ago

Developer

@phikai if the user isn't a member at all of the source project everything behaves correctly though. I understand access to the forked code can't magically be revoked but it doesn't feel normal to me that the latest commit messages can be viewed by the user who doesn't have access to that, even commits that happened after the fork.



Kai Armstrong @phikai · 9 months ago

Developer

if the user isn't a member at all of the source project everything behaves correctly though

Hmm... that is awkward.

@mnohr Can we make sure someone picks this up while we're still under allocation.



Marc Shaw @marc_shaw · 9 months ago

Maintainer

Can pick this up 🙌

Please [register](#) or [sign in](#) to reply



Dominic Couture added group `code review` `devops` `create` scoped labels 9 months ago



Dominic Couture removed `security-group-missing` `security-triage-appsec` labels 9 months ago



GitLab SecurityBot @gitlab-securitybot · 9 months ago

Author

Reporter

@phikai @mnohr @mhenriksen This issue is ready for triage as per [HackerOne process](#).

About this automation: [AppSec Escalation Engine](#)



GitLab Bot added `section` `dev` scoped label 9 months ago



Marc Shaw assigned to @marc_shaw 9 months ago



Marc Shaw @marc_shaw · 9 months ago

Maintainer

@phikai @pedroms Could I have some input here.

When we create a merge request, the default behavior for the target branch info is that the we have the parent of the forked project as the default project, and the parents default branch as the default branch.

How do we want to handle this?

I see it that this issue involves two changes.

Firstly, if the user does not have access to the parent fork, then we default to the current project, and its own default info.

Secondly, we need to change the api `branch_to` method to return 404 when the user does not have access to the merge request of the project requested.

With both of these changes, we will firstly improve the user flow, by not showing the parent project as the default info, then secondly solve the security issue where the issue can still technically request the parent projects info.

WDYT?



Kai Armstrong @phikai · 9 months ago

Developer

@marc_shaw That plan makes sense to me, but let's be mindful of tests here to make sure we're catching the right kinds of permissions that "don't have access" and not sort of globally moving things to the fork branch if you're not a member or something.

Marc Shaw @marc_shaw · 9 months ago

Maintainer

Sounds good 🙌

Pedro Moreira da Silva @pedroms · 8 months ago

Developer

[@marc_shaw](#) your proposal makes sense to me, thank you! 🙌

Please [register](#) or [sign in](#) to reply



Matt Nohr added [workflow](#) [in dev](#) scoped label 9 months ago



Dennis Tang @dennis · 8 months ago

Developer

Hi [@mnohr](#)! Since this issue is assigned and in dev, are we able to get a milestone assigned? I'm just doing some checks on issues we've committed to as part of phasing out the engineering allocation.

Matt Nohr @mnohr · 8 months ago

Developer

[@dennis](#) Thanks for catching that. [@marc_shaw](#) is working on this now and we are hoping to have it in [%14.9](#).

Thanks to [@phikai](#) for adding the milestone!

Dennis Tang @dennis · 8 months ago

Developer

Awesome, thanks for the help [@mnohr](#) [@phikai](#) [@marc_shaw](#)!

Marc Shaw @marc_shaw · 8 months ago

Maintainer

Thanks yall!

Please [register](#) or [sign in](#) to reply



Kai Armstrong changed milestone to [%14.9](#) 8 months ago



Matt Nohr added [backend](#) label 8 months ago

Matt Nohr @mnohr · 8 months ago

Developer

I am going to move this to [%14.10](#) as it is still in progress



Matt Nohr changed milestone to [%14.10](#) 8 months ago



Matt Nohr added [Deliverable](#) label 8 months ago

Marc Shaw @marc_shaw · 7 months ago

Maintainer

This is now merged, going to close this. If we need to keep it open, feel free to reopen [@mhenriksen](#) 👍



Marc Shaw closed 7 months ago

Nick Malcolm @nmalcolm · 7 months ago

Developer

This is fixed in [14.9.2](#). Closing.

GitLab SecurityBot @gitlab-securitybot · 6 months ago

Author

Reporter

[@mhenriksen](#) - this [HackerOne](#) [security](#) issue was closed 30 days ago and should be made public. Please follow [the process for disclosing security issues](#).

If the issue needs to stay confidential, please add the [keep confidential](#) label.

If you removed confidential data from the issue description before making it public, make sure that the description history entry is deleted.



Michael Henriksen made the issue visible to everyone 6 months ago

Please [register](#) or [sign in](#) to reply