

Issue system notes reveals private project path when it is closed view merge request and moved to a public project

[HackerOne report #724880](#) by ashish_r_padelkar on 2019-10-29, assigned to [@jbroullon](#):

Summary

Hello,

When issue is closed via merge request, the associated merge request ID or commit ID is visible via issue system notes to guest users. The same system note reveals full project path too when this issue is moved to public projects.

Steps to reproduce

1. Create a issue in private project
2. Create a merge request for the same.
3. Merge the merge request so that issue is closed.
4. A system note in issue is created saying `closed via merge request` or `closed via commit`

`closed via commit 82d87a827aa9edcf9911bdf71c4ecd2a951a1fe4 just now`

OR

`@justanormaluser closed via merge request !5 just now`

5. Same is visible to Guest users in issue(go to issue details) system notes which shouldnt be possible.
6. Now move this issue to public project and the same system notes reveals the full private project path from which this issue is moved from.

What is the current *bug* behavior?

Issue system notes reveals merge request ID or commit ID, may also reveal full project path when its moved

What is the expected *correct* behavior?

None of the information related to merge request or commits should be visible

Output of checks

This bug happens on GitLab.com and might be on omnibus installations too. This is verified on Gitlab.com at the time of writing the report.

Regards,
Ashish


Impact

Merge request ID, Commit ID and Project Path visible when issue is closed via merge requests

Attachments

Warning: Attachments received through HackerOne, please exercise caution!

- [Screenshot 2019-10-29 at 20.42.29.png](#)
- [Screenshot 2019-10-29 at 20.42.14.png](#)

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

Tasks  0

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](#) added [HackerOne](#) [security](#) labels [3 years ago](#)

 [GitLab SecurityBot](#) added [priority: 4](#) [severity: 4](#) scoped labels [3 years ago](#)



[GitLab SecurityBot](#) [@gitlab-securitybot](#) · [3 years ago](#)

Author

Reporter

[HackerOne comment](#) by hackerjuan :

Hello [@]ashish_r_padelkar,

Thank you for your report. Merge request IDs and commit IDs are not considered sensitive information. Regarding the private project path, I don't see it anywhere when the issue is moved to a public project. Could you add more details and evidence about this part of the report?

Best regards, GitLab Security Team



[GitLab SecurityBot](#) [@gitlab-securitybot](#) · [3 years ago](#)

Author

Reporter

[HackerOne comment](#) by ashish_r_padelkar :

Hello [@]hackerjuan ,

If you follow my steps correctly, you should be able to see the path in system notes of issue.

For eg, see this public project <https://gitlab.com/ThisIsPublicGroup/ThisIsPublicProject/issues/23>
I have moved this issue from private project to this public project. There is only one system note in there which will reveal you the private project path `groupfor/1projectfor!` there.

Regarding Merge request IDs and commit IDs are not considered sensitive information. .I mentioned this as previously such reports were considered #588876

Regards, Ashish



[GitLab SecurityBot](#) [@gitlab-securitybot](#) · [3 years ago](#)

Author

Reporter

[HackerOne comment](#) by hackerjuan :

Hello,

I have followed your steps and haven't been able to reproduce this issue, that's why I'm asking for more information. I'm not able to see any of the system notes you mentioned on your report from a guest user after moving the issue from the private project to the public one. Can you provide a video showing the steps you followed and the project configuration so we can avoid any potential confusion?

Best regards, GitLab Security Team



[GitLab SecurityBot](#) [@gitlab-securitybot](#) · [3 years ago](#)

Author

Reporter

[HackerOne comment](#) by ashish_r_padelkar :

Hello [@]hackerjuan ,

See the video at <https://vimeo.com/371557179>

Password : Gitlab@123!

Once you verify, please change the title of the report accordingly.

Regards, Ashish



[GitLab SecurityBot](#) [@gitlab-securitybot](#) · [3 years ago](#)

Author

Reporter

[HackerOne comment](#) by ashish_r_padelkar :

Hello [@]hackerjuan ,

Are you still having difficulties in reproducing this one?

Regards, Ashish



[Juan Broullon](#) added [group](#) [project management](#) [devops](#) [plan](#) scoped labels [3 years ago](#)



Juan Broullon @jbroullon · 3 years ago

Contributor

Confirmed but very low severity.

/cc @gweaver @smcgivern



Sean McGivern added `backend` label 3 years ago



GitLab Bot added `section dev` scoped label 2 years ago



Costel Maxim added `security-backlog valid` scoped label 2 years ago



Costel Maxim mentioned in issue #38281 (closed) 2 years ago



GitLab SecurityBot added `Weakness CWE-200` scoped label 2 years ago



Costel Maxim @cmaxim · 1 year ago

Developer

Bug still valid. @jlear @gweaver Due to the low severity, I think this can be closed outside of the security release. Will make the issue public once patch is released.



Gabe Weaver changed milestone to %Backlog 1 year ago



GitLab Bot added `Accepting merge requests` label 1 year ago



Costel Maxim added `security-backlog review-complete` scoped label and automatically removed `security-backlog valid` label 1 year ago



James Ritchey added `type bug` scoped label 11 months ago



Marc Shaw assigned to @marc_shaw 11 months ago



Marc Shaw @marc_shaw · 10 months ago

Maintainer

Starting to look into this now 🙌



Matt Nohr @mnohr · 10 months ago

Developer

Thanks @marc_shaw!

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



Marc Shaw @marc_shaw · 10 months ago

Maintainer

@phikai Do you have any input on what the 'correct' thing is here?

It seems like the only security issue here is that when it is moved to a public project, we expose the path to the private project, which the user may or may not have access too.

For example, as a user of the public project, I can see:

Administrator @root closed via merge request root/flight!3 in the notes, where root/flight is a private project.

Do we say Administrator @root closed via merge request hidden or do we remove the note unless the user can see the private MR

Edited by Marc Shaw 10 months ago



Kai Armstrong @phikai · 10 months ago

Developer

@marc_shaw Do you have any links/examples where I can see this. I'm also not sure if we're explicitly talking about the guest role or if we just mean non-project members in this context.

Generally, I'd guess the system note should just omit any identifying information if you don't have access to the identifying information. However, that feels like quite a complicated and slow permissions check to essentially re-check every single system note.

AFAIK - we already hide system notes for events where it's like: Mentioned in XXX if you don't have access to that project. I'd suspect in this case it's simpler to just do that as well vs. trying to do alternate style system notes.



Marc Shaw @marc_shaw · 10 months ago

Maintainer

To follow on from this, there was a bug that was stopping this behaving consistently as in when we have other references that should be hidden. The MR resolves is 👍

Edited by [Marc Shaw](#) 10 months ago

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



Marc Shaw added [workflow](#) [in review](#) scoped label 10 months ago



GitLab Bot added [bug](#) [vulnerability](#) scoped label 10 months ago



Marc Shaw added [workflow](#) [awaiting security release](#) scoped label and automatically removed [workflow](#) [in review](#) label 9 months ago



Marc Shaw @marc_shaw · 9 months ago

Maintainer

MR is merged and should be in the latest security release



Andrew Kelly @ankelly · 9 months ago

Developer

This was fixed in 14.7.1 and assigned CVE-2022-0344

Edited by [Andrew Kelly](#) 9 months ago



Andrew Kelly closed 9 months ago



Matt Nohr changed milestone to [%14.7](#) 8 months ago



GitLab SecurityBot @gitlab-securitybot · 8 months ago

Author

Reporter

[@cmxim](#) - 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.



Costel Maxim made the issue visible to everyone 8 months ago

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