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

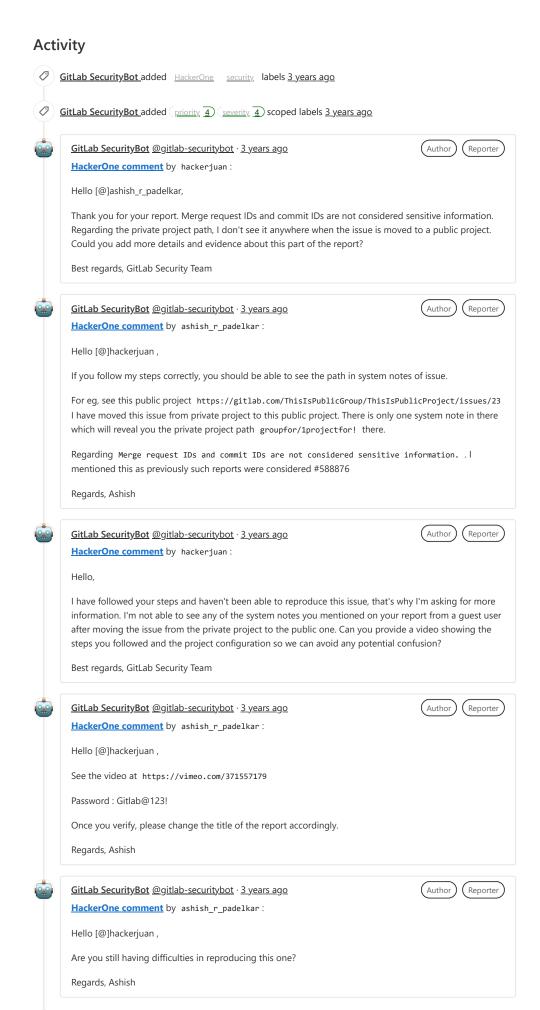
Attachments

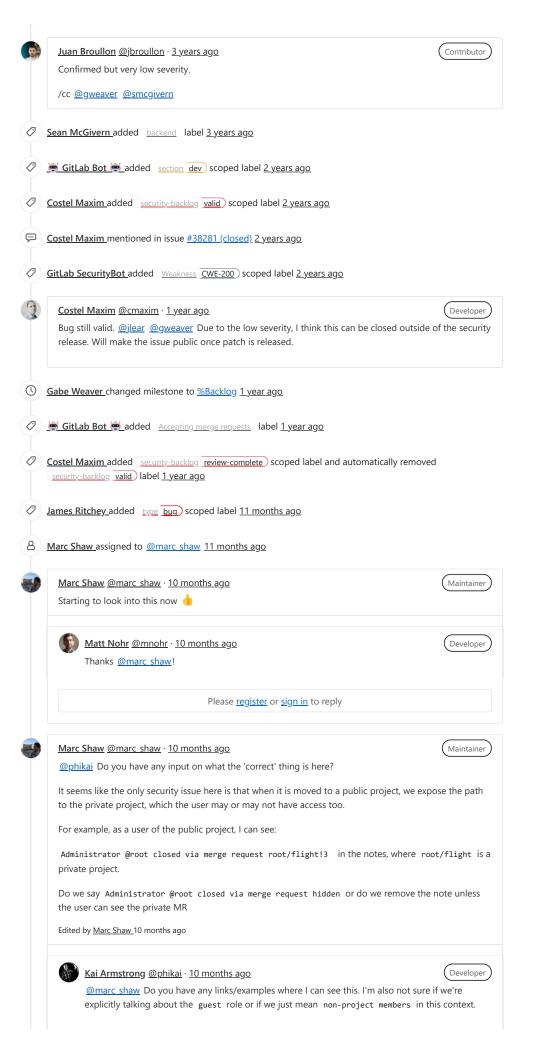
Warning: Attachments received through HackerOne, please exercise caution!

- Screenshot 2019-10-29 at 20.42.29.png
- Screenshot 2019-10-29 at 20.42.14.png

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

Tasks 0	
No tasks are currently assigned. Use tasks to break down this issue into smaller parts.	
III III Da	
Linked items 0	
Link issues together to show that they're related or that one is blocking others. <u>Learn more.</u>	





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. (Maintainer Marc Shaw @marc shaw · 10 months ago 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 <u>register</u> or <u>sign in</u> to reply Marc Shaw added workflow in review scoped label 10 months ago (a) 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 Maintaine 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 (1) Matt Nohr changed milestone to <u>%14.7</u> 8 months ago Reporter <u>GitLab SecurityBot</u> @gitlab-securitybot · 8 months ago @cmaxim - 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