Closed · Issue created 2 years ago by GitLab SecurityBot

Unauthorized access to private project security dashboard

HackerOne report #853355 by vaibzsvicky on 2020-04-19, assigned to @dcouture:

Summary

User with guest permissions can't view security dashboard of the private project. However, this is not applied when user permission changes from maintainer to guest.

As a result, if user was previously a maintainer in the project he/she can add the project to their security dashboard and when their access levels decreases to guest, they can still view new security vulnerabilities result found in the project through their security dashboard. New security issues found in the project are reflecting back to the guest user security dashboard.

Steps to reproduce

- User A create a private project and add user B with maintainer access
- User B will add the project in his security dashboard.
- User A reduced the user B access level to guest. Now, user B can't view any old and new security issues in the project directly
- User B access the project new as well as old security issues through his security dashboard and also the specific new files where the issues lies
- Done

Impact

The impact of this vulnerability is actually very high. A malicious user can take advantage of the security issues found and can use it to exploit the owner application. **More info** will also disclose newly added files, dependencies and new internal structure of the project/application to the unauthorized user.

What is the current *bug* behavior?

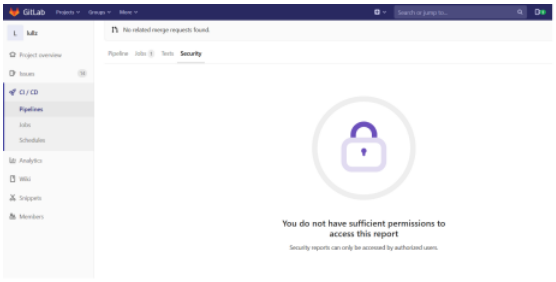
Unauthorized user (guest) can view security dashboard of the private project

What is the expected *correct* behavior?

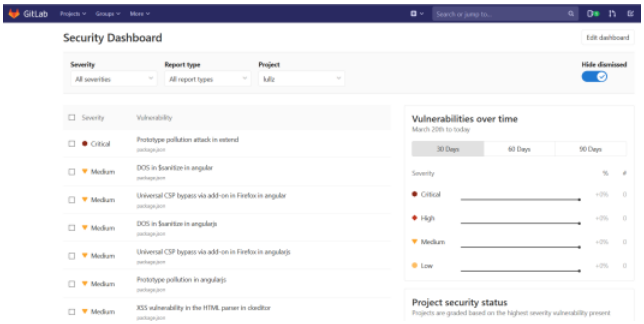
Project should be removed from the user security dashboard when his/her permission changes to lower.

Relevant logs and/or screenshots

When permission changes to guest, user can't view the security dashboard directly, they are treated with this message.



But user can access the private project security issues through his own security dashboard.



Output of checks

This bug happens on GitLab.com

NOTE : I'm using one of the example project provided by Gitlab named "yarn-vulnerabilities" for security testing.
If you want to quickly validate my report, please consider using it. https://gitlab.com/gitlab-examples/security/yarn-vulnerabilities.

Thanks,
Vaibhav Singh

Impact

Unauthorized access to private project security dashboard which allows a malicious user to exploit the owner application and also disclose application newly added files/dependencies and internal structure.

Attachments

Warning: Attachments received through HackerOne, please exercise caution!

- sec1.png
- sec2.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 1

Relates to

Limit access to the instance security dashboard #38383 · Backlog

Activity

GitLab SecurityBot added priority 4 severity 4 scoped labels 2 years ago

GitLab SecurityBot added HackerOne security labels 2 years ago

GitLab SecurityBot @gitlab-securitybot · 2 years ago · Author · Reporter
HackerOne comment by vaibzsvicky :

Steps to reproduce using Gitlab example project "yarn-vulnerabilities" ,

https://gitlab.com/gitlab-examples/security/yarn-vulnerabilities

- Create an empty private project and add user B as maintainer
- User B add project to its profile security dashboard
- Change the permission of user B to guest. Now, user B can't view security dashboard of the project
- Upload `.gitlab-ci.yml` and `package.json` of "yarn-vulnerabilities" to your project.
- Pipeline will run automatically, after it is finish, it will report 1 critical, 8 medium and 8 low security issues
- Login to user B account, go to your security dashboard, you'll see all new vulnerabilities found in the project is reflected back to you. (guest user)

GitLab SecurityBot @gitlab-securitybot · 2 years ago Author Reporter

HackerOne comment by `dcouture` :

Doesn't look critical

GitLab SecurityBot @gitlab-securitybot · 2 years ago Author Reporter

HackerOne comment by `dcouture` :

More simple repro steps

1. Fork `https://gitlab.com/gitlab-examples/security/yarn-vulnerabilities` as `user A` and make it private
2. Trigger a pipeline so there are security scan results
3. Invite `user B` as maintainer
4. Add the project to your instance dashboard at https://gitlab.com/-/security/
5. Change `user B` to guest
6. Notice `user B` cannot see the dashboard in the project anymore but they still see the results in their instance dashboard

Interesting fact: if you remove the user from the project the dashboard disappears, but if you add them back as guest it will reappear.

GitLab SecurityBot @gitlab-securitybot · 2 years ago Author Reporter

HackerOne comment by `dcouture` :

Hi [@]vaib25vicky,

Thank you for submitting this report. I could reproduce the issue and indeed the `Use security dashboard` permission should be restricted to users that are in the `Developer` role or above. However I would like you to elaborate on the impact. Keeping in mind that:

- This vulnerability can only be exploited by an ex-maintainer that turns against their old project
- There is no way to target an arbitrary project
- The attacker doesn't have access to the code or the issues, only the name of the files and vulnerabilities
- The attacker already had access to the vulnerability list and code previously and really only the new issues will potentially be disclosed

I believe the impact for this is very limited. If you disagree, can you please provide an attack scenario that would demonstrate the higher impact?

Best regards, Dominic GitLab Security Team

GitLab SecurityBot @gitlab-securitybot · 2 years ago Author Reporter

HackerOne comment by `vaib25vicky` :

Hi,

Attack Scenario:

- Project is in initial stage, admin added maintainers to help it grow
- Admin make some maintainers to lower access so that they can't access sensitive information
- One of the maintainer/attacker exploit this vulnerability, and access newly added security issues
- With the newly added security issues found in the project, attacker exploit the project/application

I agreed to your points above, the reason I consider this critical because disclosing the security issues to unauthorized users make the application/project vulnerable to exploitation by the attacker. I think it is more crucial to not disclose security issues in the project to others than code or issues.

But feel free to adjust the severity of the report to medium/high, if you feel otherwise.

Thanks

Dominic Couture @dcouture · 2 years ago Developer

Seems like fixing this bug would solve this issue I found while looking for duplicates

GitLab SecurityBot added security-group-missing security-triage-appsec labels 2 years ago

Dominic Couture @dcouture · 2 years ago Developer

Hello @sethgitlab and @derekferguson ! A reporter has found a permission issue in the instance dashboard where users can see a project dashboard even with insufficient rights after being "demoted" to guest.

Dominic Couture added group dynamic analysis devops secure priority 3 severity 3 scoped labels and automatically removed priority 4 severity 4 labels 2 years ago

Seth Berger added security dashboard label 2 years ago

Matt Wilson changed milestone to %13.1 2 years ago

Matt Wilson added group threat insights type bug devops protect scoped labels and automatically removed group dynamic analysis devops secure labels 2 years ago

GitLab SecurityBot removed security-group-missing security-triage-appsec labels 2 years ago

GitLab SecurityBot changed due date to July 19, 2020 2 years ago

GitLab Bot added Accepting merge requests label 2 years ago

Wayne Haber added workflow scheduling scoped label 2 years ago

Seth Berger marked this issue as related to #38383 2 years ago

Seth Berger mentioned in issue #215570 (closed) 2 years ago

Lindsay Kerr @lkerr · 2 years ago Contributor

@minac can you please take a look at this issue from a *refinement* perspective? Let me know if there is any frontend work required, and also what the weight would be for the backend work required?

Mehmet Emin INAC @minac · 2 years ago Maintainer

Hi @lkerr, 👋 I can reproduce the issue locally but only for the old dashboard. FCV dashboard does not have this problem(`Project security status` card shows the project though). But regardless of this information, we should fix project_authorizations method we have in `InstanceSecurityDashboard` model. The fix seems trivial; just scope the query to ignore `guest` permission levels.

I've also tried to add a project with guest role via manage dashboard page and found out that the search results had the project but couldn't add the project to my dashboard.

There is no frontend work required to fix this issue. I'm adding backend-weight 3 .

Please register or sign in to reply

Lindsay Kerr added workflow refinement scoped label and automatically removed workflow scheduling label 2 years ago

Lindsay Kerr assigned to @minac 2 years ago

GitLab Bot removed Accepting merge requests label 2 years ago

Mehmet Emin INAC added backend-weight 3 scoped label 2 years ago

Mehmet Emin INAC added workflow scheduling scoped label and removed workflow refinement backend-weight 3 labels 2 years ago

Mehmet Emin INAC @minac · 2 years ago — Maintainer

I've updated the workflow label as `workflow::scheduling` and assigning this to @matt_wilson to prioritize(I assume this must be high priority though).

> **Mehmet Emin INAC** @minac · 2 years ago — Maintainer
>
> I just realized this has been already prioritized so I am updating the label as `workflow::ready for development`.
>
> Please register or sign in to reply

Mehmet Emin INAC added `workflow::ready for development` scoped label and automatically removed `workflow::scheduling` label 2 years ago

Mehmet Emin INAC unassigned @minac 2 years ago

GitLab Bot added `Accepting merge requests` label 2 years ago

Lindsay Kerr changed weight to **3** 2 years ago

Lindsay Kerr added `backend` label 2 years ago

Lindsay Kerr mentioned in issue gitlab-org/defend/general#718 2 years ago

Mehmet Emin INAC assigned to @minac 2 years ago

Mehmet Emin INAC added `workflow::in dev` scoped label and automatically removed `workflow::ready for development` label 2 years ago

Mehmet Emin INAC @minac · 2 years ago — Maintainer

@dcouture - I've prepared the change and even pushed the branch but before opening the MR, I realized that this might be a problem since the issue is confidential and deleted the branch. How do we apply the patch I've created for this issue?

/cc @thiagocsf

Edited by Mehmet Emin INAC 2 years ago

> **Dominic Couture** @dcouture · 2 years ago — Developer
>
> Hi @minac, please follow this procedure to open your MR and security issue in the https://gitlab.com/gitlab-org/security/gitlab/ repository.
>
> Please register or sign in to reply

Mehmet Emin INAC mentioned in issue #38383 2 years ago

GitLab Bot removed `Accepting merge requests` label 2 years ago

Mehmet Emin INAC added `workflow::in review` scoped label and automatically removed `workflow::in dev` label 2 years ago

GitLab Bot @gitlab-bot · 2 years ago — Maintainer

Setting `Category:Vulnerability Management` based on `group::threat insights`.

GitLab Bot added `Category:Vulnerability Management` label 2 years ago

Mehmet Emin INAC @minac · 2 years ago — Maintainer

The MRs to fix this issue has been merged into master and security release branches on security project;

- Master: https://gitlab.com/gitlab-org/security/gitlab/-/merge_requests/561
- 13-1-stable-ee: https://gitlab.com/gitlab-org/security/gitlab/-/merge_requests/585
- 13-0-stable-ee: https://gitlab.com/gitlab-org/security/gitlab/-/merge_requests/583
- 12.10-stable-ee: https://gitlab.com/gitlab-org/security/gitlab/-/merge_requests/584

Edited by Mehmet Emin INAC 2 years ago

GitLab SecurityBot added `security-issue-escalated` label 2 years ago

GitLab SecurityBot @gitlab-securitybot · 2 years ago — Author — Reporter

@mattdw @thiagocsf @lindsay_kerr @nqeorge1 This ~S3 `security` issue's milestone has expired.

About this automation: AppSec Escalation Engine

Thiago Figueiró added `workflow::verification` scoped label and automatically removed `workflow::in review` label 2 years ago

Costel Maxim @cmaxim · 2 years ago — Developer

Issue fixed in 13.1.2

Costel Maxim closed 2 years ago

GitLab SecurityBot removed `security-issue-escalated` label 2 years ago

GitLab SecurityBot @gitlab-securitybot · 2 years ago — Author — Reporter

This `HackerOne` `security` issue was closed 30 days ago and may become public.

Please ensure the following items are true and add a ✅ reaction:

- Issue description and comments do not contain sensitive data belonging to GitLab.
- Issue does not reveal private information of the reporter (i.e. session IDs, passwords).

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 @cmaxim · 2 years ago — Developer

Making issue public.

Costel Maxim made the issue visible to everyone 2 years ago

GitLab SecurityBot @gitlab-securitybot · 2 years ago — Author — Reporter

HackerOne report #853355 was disclosed on 2020-11-21 @ 02:22.

- Bounty awarded: $2000

Please register or sign in to reply