Closed · Issue created 3 years ago by GitLab SecurityBot

Endpoint for auto-completing Assignee discloses the members of private groups

HackerOne report #627507 by `ngalog` on 2019-06-24, assigned to `estrike`:

Summary

I have a project, with id `10257668`, and I have invited a private group as a developer to this project. As that group is private, you should not see its membership. However, there is a way to find out project's private membership:

- Correct permission check: https://gitlab.com/api/v4/projects/:project_id/members - does not disclose private group's membership.
- Incorrect permission check: https://gitlab.com/autocomplete/users.json?search=&active=true&project_id=10257668&current_user=true - discloses the members of private group.

Steps to reproduce:

1. Login to gitlab.com.
2. Visit this project members page: https://gitlab.com/api/v4/projects/10257668/members. See this project has only one member.
3. Visit https://gitlab.com/autocomplete/users.json?search=&active=true&project_id=10257668&current_user=true. See this project has more than one member, thus disclosing the private membership.

Impact

Disclosure of members in a private group.

Proposal

The autocomplete endpoint should use the permission check from the Project Members API endpoint (`https://gitlab.com/api/v4/projects/[project-id]/members`).

Edited 1 year ago by Dan Jensen

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.

Related merge requests 1

Add membership CSV export to root group [RUN-AS-IF-FOSS] [RUN ALL RSPEC]

!66755 · 14.2

Activity

GitLab SecurityBot added HackerOne security labels 3 years ago

GitLab SecurityBot added security-sp-label-missing security-triage-appsec labels 3 years ago

Ethan Strike added group optimize devops manage priority 3 severity 3 scoped labels 3 years ago

Ethan Strike added Manage [DEPRECATED] label and removed security-sp-label-missing security-triage-appsec labels 3 years ago

Ethan Strike changed due date to September 23, 2019 3 years ago

Ethan Strike @estrike · 3 years ago — Developer

This is similar to gitlab-ce#53011, but the information is disclosed through a different endpoint (/autocomplete/users.json) that uses different logic (https://gitlab.com/gitlab-org/gitlab-ce/blob/master/app/controllers/autocomplete_controller.rb#L6).

As in the previous issue, the situations is as follows:

- The project is public
- A private group is invited to the project
- The endpoint discloses the members of the private to a user that is neither a member of the project or the private group

The visibility should be according to this comment from Jeremy: https://gitlab.com/gitlab-org/gitlab-ce/issues/53011#note_181442691

Please let me know if this is considered a duplicate.

/cc @valexieva @lmcandrew

Edited by Ethan Strike 3 years ago

GitLab SecurityBot assigned to @valexieva 3 years ago

GitLab SecurityBot @gitlab-securitybot · 3 years ago — Author · Reporter

This security issue is currently unassigned, assigning the group PM according to the `group::` label.

Please `/reassign`, if possible.

More information: https://gitlab.com/gitlab-com/gl-security/engineering/issues/446

Virjinia Alexieva changed milestone to %12.6 3 years ago

Virjinia Alexieva added devops plan scoped label and automatically removed devops manage label 3 years ago

Virjinia Alexieva added group project management scoped label and automatically removed group optimize label 3 years ago

Virjinia Alexieva added group authentication and authorization scoped label and automatically removed group project management label 3 years ago

Virjinia Alexieva added devops manage scoped label and automatically removed devops plan label 3 years ago

Juan Broullon mentioned in issue gitlab-ce#65191 3 years ago

Juan Broullon marked this issue as related to gitlab-ce#65191 3 years ago

GitLab Bot changed due date to September 23, 2019 3 years ago

GitLab Bot changed milestone to %12.6 3 years ago

GitLab Bot moved from gitlab-ce#63714 3 years ago

Virjinia Alexieva assigned to @jeremy and unassigned @valexieva 3 years ago

Jeremy Watson (ex-GitLab) @jeremy-gl · 3 years ago — Contributor

@mksionek, do you consider this a duplicate of #24822 (closed)?

Gosia Ksionek @mksionek · 3 years ago — Developer

no, it's not, it is identical problem, but touching different parts of code.

Jeremy Watson (ex-GitLab) changed milestone to %12.9 3 years ago

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

Setting Category:Authentication and Authorization based on ~"group::access".

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

Setting Category:Authentication and Authorization based on ~"group::access".

GitLab Bot added Category:Authentication and Authorization label 2 years ago

Jeremy Watson (ex-GitLab) changed milestone to %13.0 2 years ago

Michelle Gill mentioned in issue gitlab-com/Product#624 (closed) 2 years ago

Jeremy Watson (ex-GitLab) changed milestone to %13.12 2 years ago

Michelle Gill @m_gill · 2 years ago — Developer

@johnhope is this actually devops plan?

John Hope @johnhope · 2 years ago — Developer

@m_gill Sorry for the delayed response. This one's to do with members in projects/groups so I think it should stay with ~"group::access". Looks like they fixed something similar so they may have the context too.

Please register or sign in to reply

GitLab Bot added section dev scoped label 2 years ago

Ron Chan added security-backlog valid scoped label 2 years ago

GitLab SecurityBot added Weakness CWE-284 scoped label 2 years ago

Liam McAndrew added Category:User Management label 1 year ago

Liam McAndrew removed Category:Authentication and Authorization label 1 year ago

Dan Jensen unassigned @jeremy-ql 1 year ago

GitLab Bot added Accepting merge requests label 1 year ago

Dan Jensen added workflow planning breakdown scoped label 1 year ago

Dan Jensen added backend label 1 year ago

Dan Jensen removed milestone 1 year ago

Dan Jensen changed the description 1 year ago

Dan Jensen changed weight to 2 1 year ago

Dan Jensen added workflow scheduling scoped label and automatically removed workflow planning breakdown label 1 year ago

Dan Jensen added 1 deleted label 1 year ago

Dan Jensen added Epic 6340 label 1 year ago

GitLab Bot @gitlab-bot · 1 year ago — Maintainer

Setting label(s) Category:Authentication and Authorization based on ~"group::access".

GitLab Bot added Category:Authentication and Authorization label 1 year ago

Magdalena Frankiewicz assigned to @m_frankiewicz 1 year ago

GitLab Bot removed Accepting merge requests label 1 year ago

Dan Jensen changed milestone to %14.2 1 year ago

Dan Jensen added workflow ready for development scoped label and automatically removed workflow scheduling label 1 year ago

Dan Jensen removed Manage [DEPRECATED] label 1 year ago

Magdalena Frankiewicz @m_frankiewicz · 1 year ago — Developer

Note: the url is now https://gitlab.com/-/autocomplete/users.json?search=&active=true&project_id=10257668&current_user=true

Magdalena Frankiewicz @m_frankiewicz · 1 year ago — Developer

I'm trying to wrap my head around this issue and what the expected behavior here would be, and I'd appreciate help from people with more context on it, maybe @mksionek, @manojmj or @estrike?

I started with checking the urls from issue description; I can see differences described above differences: when I'm logged in to GitLab.com https://gitlab.com/api/v4/projects/10257668/members returns info on one user only:

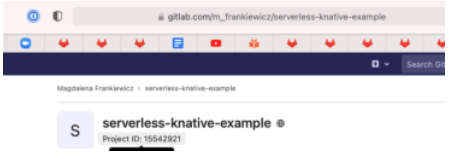
```
[{"id":3383044,"name":"rontest1","username":"rontest1","state":"active","avatar_url":"https://secure.gravatar.com
```

while https://gitlab.com/-/autocomplete/users?search=&active=true&project_id=10257668&current_user=true lists more users, my user included:

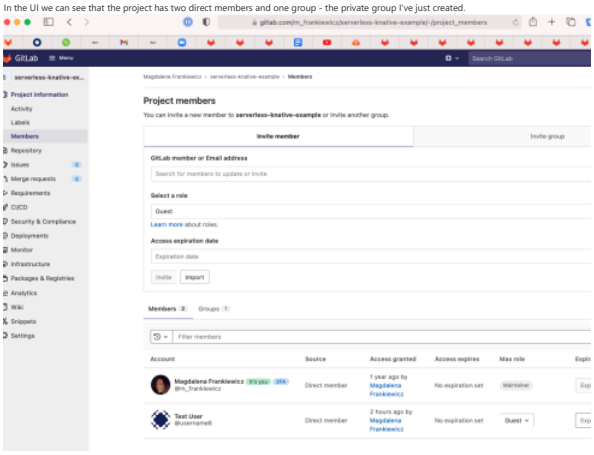
```
[{"id":4826728,"name":"Magdalena Frankiewicz","username":"m_frankiewicz","state":"active","avatar_url":"https://s
```

What is more, when checking urls in **incognito** mode, the first url returns `401 Unauthorized`, while the second one returns same result minus my user.

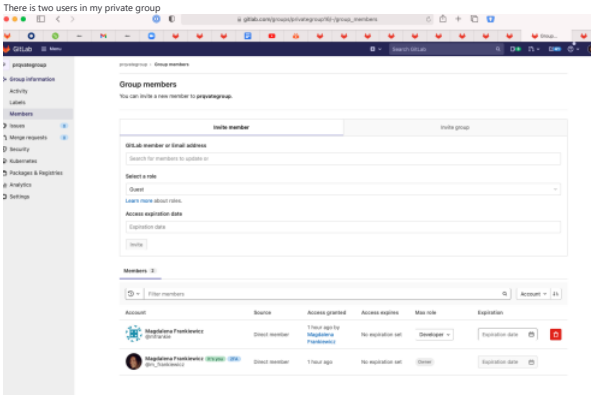
To better understand the current behavior I created a private group and invited it to a public project that I'm a Maintainer on: `serverless-knative-example` with ID 15542921



In the UI we can see that the project has two direct members and one group - the private group I've just created.



There is two users in my private group



The autocomplete url for this project users returns 3 members **both** when I'm logged in and in incognito mode, so it shows the user who is part of the private group.

https://gitlab.com/api/v4/projects/15542921/members returns 2 users (like UI) when I'm logged in and `401` in incognito.

This confirms that `autocomplete` endpoint returns information on all users, also private, to anyone that has a project ID.

What should happen here? It seems that `autocomplete` endpoint is used also in situations, that do not require user authentication:

```
class AutocompleteController < ApplicationController
  skip_before_action :authenticate_user!, only: [:users, :award_emojis, :merge_request_target_branches]
...
end
```

Gosia Ksionek @mksionek · 1 year ago Developer

@m_frankiewicz I believe this comment: gitlab-foss#53011 (comment 181442691) from Jeremy still stands. But as I see in the code, it would be a huge change to filter out members of private group (because we use this: https://gitlab.com/gitlab-org/gitlab/blob/master/app/models/project.rb#L250-250)

Magdalena Frankiewicz @m_frankiewicz · 1 year ago Developer

Thanks for reply @mksionek . Is seeing any data when checking in incognito mode `https://gitlab.com/-/autocomplete/users?search=&active=true&project_id=[project_id]&current_user=true` a correct behavior?

Gosia Ksionek @mksionek · 1 year ago Developer

From the Git history I would say it is a really old behaviour... hard to say what was the reasoning behind it.

But when we have public project, we can go to the members page and see all the members, so I would say that there is nothing dangerous about it, apart from the behaviour described in the issue.

WDYT @m_frankiewicz ??

Magdalena Frankiewicz @m_frankiewicz · 1 year ago Developer

Right @mksionek , and that would mean, that there should be user authentication on the `autocomplete` endpoint, otherwise how do we know if the user is a member of the private group? The endpoint should try to authenticate, in case it's not possible, it could return minimum access information. The question here is, if there is a good reason to skip authentication, as it was done in the first place.

On top of Jeremy's comment there are some other cases that should be clarified, e.g. should the project `Owner` of the shared project be able to see the members of the private group, even if they don't belong to it?

Could @ogolowinski help answer those questions?

Orit Golowinski @ogolowinski · 1 year ago Developer

@m_frankiewicz can an `owner` not be part of the private group?

Gosia Ksionek @mksionek · 1 year ago Developer

@ogolowinski Yes, if there are more owners and only one of them are the member of invited private group.

@m_frankiewicz but currently we can invoke `current_user` in this endpoint, so we can use it in a context that you've described.

I believe the only reason to skip it is if some place that uses this endpoint is not requiring being logged in. I think it should not be a problem to list those places.

Gosia Ksionek @mksionek · 1 year ago Developer

@m_frankiewicz regarding projects we have this kind of documentation: https://docs.gitlab.com/ee/user/project/members/share_project_with_groups.html#sharing-public-project-with-private-group

we were also dealing with similar problem here: https://dev.gitlab.org/gitlab/gitlabhq/-/merge_requests/3212/diffs#diff-content-25c9a4388d380a2dcd439cec2b346a25d1078264

Ethan Strike @estrike · 1 year ago Developer

@rshambhuni Can you take this over for me as stable counterpart for this group?

Rohit Shambhuni @rshambhuni · 1 year ago Developer

@estrike Absolutely. I'll take a look at the issue and this discussion.

Please register or sign in to reply

Magdalena Frankiewicz @m_frankiewicz · 1 year ago Developer

Is the title of the issue correct?

Dan Jensen @djensen · 1 year ago Contributor

@m_frankiewicz good question, it was a bit difficult to understand. I just updated it, what do you think now?

Please register or sign in to reply

GitLab Bot mentioned in issue gitlab-org/quality/triage-reports#4196 (closed) 1 year ago

Gosia Ksionek mentioned in merge request !66755 (merged) 1 year ago

Dan Jensen changed title from **Disclosure of private membership in Issues Assignee** to **Endpoint for auto-completing Assignee discloses the members of private groups** 1 year ago

Dan Jensen changed the description 1 year ago

Sanad Liaquat added quad-planning complete-no-action scoped label 1 year ago

Gosia Ksionek mentioned in issue gitlab-org/manage/access/discussion#18 1 year ago

Michelle Gill added FY22 Q3 scoped label 1 year ago

Dennis Tang changed milestone to %14.3 1 year ago

Dennis Tang added missed:14.2 missed-deliverable labels 1 year ago

Magdalena Frankiewicz added workflow in dev scoped label and automatically removed workflow ready for development label 1 year ago

Dan Jensen changed the description 1 year ago

Magdalena Frankiewicz added workflow in review scoped label and automatically removed workflow in dev label 1 year ago

Magdalena Frankiewicz changed weight to **3** 1 year ago

Michelle Gill added to epic &6636 1 year ago

GitLab SecurityBot added security-issue-escalated label 1 year ago

GitLab SecurityBot @gitlab-securitybot · 1 year ago Author Reporter

@hsutor @dennis @lmcandrew @rshambhuni This severity 3 security issue's milestone has expired.

About this automation: AppSec Escalation Engine

Hannah Sutor changed milestone to %14.4 1 year ago

Hannah Sutor @hsutor · 1 year ago Developer

Changed milestone to %14.4

Hannah Sutor removed due date 1 year ago

Magdalena Frankiewicz added workflow blocked scoped label and automatically removed workflow in review label 1 year ago

Magdalena Frankiewicz @m_frankiewicz · 1 year ago Developer

As the MR for this is blocked https://gitlab.com/gitlab-org/security/gitlab/-/merge_requests/1687#note_680468967, I'm also removing the milestone for now.

Magdalena Frankiewicz removed milestone 1 year ago

Michelle Gill added group workspace scoped label and automatically removed group authentication and authorization label 1 year ago

Dan Jensen added bug bug scoped label 1 year ago

Rohit Shambhuni removed security-backlog valid label 1 year ago

Rohit Shambhuni added security-backlog review-complete scoped label 1 year ago

Rohit Shambhuni changed due date to February 28, 2022 11 months ago

Magdalena Frankiewicz changed milestone to %14.3 11 months ago

Hannah Sutor removed workflow blocked label 11 months ago

Hannah Sutor closed 11 months ago

Hannah Sutor @hsutor · 11 months ago Developer

Summary of this issue:

When sharing a private group into a private project, I can see its members using the autocomplete endpoint and I don't think I should be able to.

Why I closed it: When you share a private group into a private project, any members of the project can then see the members of the group. Therefore, this is not a bug.

Link to further discussion: https://gitlab.com/gitlab-org/security/gitlab/-/merge_requests/1687#note_803573407

GitLab SecurityBot removed security-issue-escalated label 11 months ago

GitLab SecurityBot @gitlab-securitybot · 10 months ago Author Reporter

@rshambhuni - 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.

Rohit Shambhuni made the issue visible to everyone 10 months ago

Christina Lohr mentioned in epic gitlab-org/manage/authentication-and-authorization&1 (closed) 6 months ago

Christina Lohr mentioned in issue #364280 (closed) 6 months ago

Christina Lohr mentioned in epic &8184 6 months ago

Please register or sign in to reply