Closed · Issue created 3 years ago by GitLab SecurityBot

Import pending members from public projects or private projects (if you have guest role)

HackerOne report #542539 by `ashish_r_padelkar` on 2019-04-19, assigned to `asaba`:

Summary

Hello,

As per documentation here `https://docs.gitlab.com/ee/user/project/members/#import-users-from-another-project` ,

`In the dropdown menu, you can see only the projects you are Maintainer on`.

This is NOT true. You can also see the projects where you have just `Guest` access to.

The problem with this is, once you import members from such projects, a guest can see all pending members who are invited using emails but havent joined the project yet! i.e guests will be able to see all the email ids of the members who are invited using email by Admins but not yet joined gitlab.

If they just visit the url directly in UI, they dont see these members who have not joined gitlab yet!

Steps to reproduce

1. As a Owner in your project, navigate to `https://gitlab.com/<YourUserName>/<YourProject>/project_members/import`
2. When you click on the dropdown, you will not only see the projects where you are maintainer on, but you will see all the projects where you just have `Guest` role too.
3. Select the project where you have `Guest` role and click on `Import Project Members`.

The Request responsible for this is

```
POST /<YourUserName>/<YourProject>/project_members/apply_import HTTP/1.1
Host: gitlab.com
Connection: close
Content-Length: 157
Cache-Control: max-age=0
Origin: https://gitlab.com
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.103 Saf
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v
Referer: 1
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie: 1

utf8=%E2%9C%93&authenticity_token=1&source_project_id=10776018
```

4. You can also replace the `source_project_id` parameter in above request with public projects too, and it will import from public projects too!
5. This will import the email ids of member who have not joined the selected project which you dont see when you navigate to member url from UI!

Examples POC

Navigate to my public project here `https://gitlab.com/gitlabadminrsspl1111/thisispublicproject/project_members`

You will just see one member there.

Now follow the above reproduction steps, and replace the `source_project_id` parameter in above request to `10776018` and send the request

Now check the member list. You will see an email there . This is an invited email which guest users cant see normally as the invited member has not yet joined the gitlab/project!

What is the current *bug* behavior?

Allows you to import pending members from public projects as well as private projects where you just have guest role

What is the expected *correct* behavior?

Only members from project which you have maintainers role should be allowed to import

Output of checks

This bug happens on GitLab.com and might be on omnibus installations too

Impact

Allows you to import pending members from public projects as well as private projects where you just have guest role.

Proposal

The `Import` feature should only allow users to import members from projects where the user has a `Maintainer` role. This should address issues called out under steps 2 and 4 under **Steps to Reproduce** section.

Edited 1 year ago by Rohit Shambhuni

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 3 severity 3 scoped labels 3 years ago

GitLab SecurityBot @gitlab-securitybot · 3 years ago (Author) (Reporter)
HackerOne comment by `ashish_r_padelkar`:

Note that you dont need any permissions in public projects to get this work

Antony Saba added Manage [DEPRECATED] label 3 years ago

Antony Saba added 1 deleted label 3 years ago

Antony Saba changed due date to July 23, 2019 3 years ago

Antony Saba @asaba · 3 years ago (Contributor)
cc @jeremy

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

Ethan Strike added group authentication and authorization scoped label 3 years ago

Ethan Strike added group optimize scoped label and automatically removed group authentication and authorization label 3 years ago

GitLab SecurityBot removed security-group-missing security-triage-appsec labels 3 years ago

GitLab SecurityBot assigned to @valexieva 3 years ago

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

This security issue has no milestone with a start date.

Assigning the group PM according to the `group::` label. Please set a milestone with a start date.

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

Virjinia Alexieva changed milestone to %12.7 3 years ago

Virjinia Alexieva added project label 3 years ago

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

Rémy Coutable added Category:Subgroups label 3 years ago

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

Jeremy Watson (ex-GitLab) removed Manage (DEPRECATED) label 3 years ago

GitLab Bot @gitlab-bot · 3 years ago — Maintainer

Setting gitlab-ce~~#116795 based on gitlab-ce~~10046105.

GitLab Bot added devops manage scoped label 3 years ago

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

GitLab Bot changed milestone to %12.7 3 years ago

GitLab Bot moved from gitlab-ce#61267 3 years ago

Jeremy Watson (ex-GitLab) unassigned @jeremy 3 years ago

Jeremy Watson (ex-GitLab) changed milestone to %13.0 3 years ago

GitLab Bot added Accepting merge requests label 3 years ago

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

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

Mark Fletcher removed group authentication and authorization label 2 years ago

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

Setting ~"group::spaces" based on Category:Subgroups .

GitLab Bot added group spaces DEPRECATED scoped label 2 years ago

Luca Kisielius added estimation needed scoped label 2 years ago

Luca Kisielius added Deliverable label 2 years ago

GitLab Bot removed Deliverable label 2 years ago

Luca Kisielius changed milestone to %Backlog 2 years ago

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

Setting ~"group::access" based on Category:Subgroups .

GitLab Bot added group authentication and authorization scoped label and automatically removed group spaces DEPRECATED label 2 years ago

GitLab Bot added section dev scoped label 2 years ago

Ron Chan @rchan-gitlab · 2 years ago — Contributor

/cc @lmcandrew for visibility

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

GitLab SecurityBot added Weakness CWE-285 scoped label 2 years ago

Ron Chan @rchan-gitlab · 1 year ago — Contributor

@ngeorge1 Just want to get more opinion on this one, recently we received a report from the same reporter that they could see invited email for public groups https://hackerone.com/reports/1048259

And we later decided the risk is very small and not worth fixing it, and that's why we are currently at this issue and want to do the same about this finding, by closing this issue here as Informative and make it a public issue.

WDYT?

cc @dcouture

Edited by Ron Chan 1 year ago

Ron Chan @rchan-gitlab · 1 year ago — Contributor

Also cc @lmcandrew if you have any thoughts on this

Nikhil George @ngeorge1 · 1 year ago — Developer

@rchan-gitlab: I think it is fine to close the #542539 H1 report `Informative` considering the low-security impact. Between, do we make the severity 4 issue public before fixing it? My impression was all the security issues stay `confidential` until it is fixed.

Dominic Couture @dcouture · 1 year ago — Developer

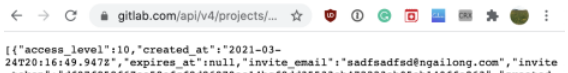
Depends on if we view it as a vulnerability or just a security enhancement.

I think if we're not ready to make this public then we should accept keep the H1 report opened. With that being said, the list of pending users I think isn't a problem but I'm seeing this mentions emails here.

If it leaks email addresses then perhaps it's a valid security issue. Does the new report also leak email addresses?

Ron Chan @rchan-gitlab · 1 year ago — Contributor

@dcouture yes the new report also "leak" email addresses, for example, does it change your mind to accept the report https://hackerone.com/reports/1048259? The email address of the invitee could be changed after accepting the invitation, since it could be accepted by an user with a different email address, so the email address could be just a temporary email for receiving the email, or could be their real email address too.




```
[{"access_level":10,"created_at":"2021-03-24T20:16:49.947Z","expires_at":null,"invite_email":"sadfsadfsd@ngailong.com","invite_token":"df97f858f67ea58efcf8d86879ae14bcf8dd35533eb472223ab05ab140ffe863","created_by_name":"Ron Chan"}]
```


This makes me wonder if the invite_token is a sensitive information leak

Edited by Ron Chan 1 year ago

Ron Chan @rchan-gitlab · 1 year ago — Contributor

After investigating for a while, I can't exploit it because I can't find an endpoint to apply the invite_token during the member confirmation step

Dominic Couture @dcouture · 1 year ago — Developer

Hmm in that case @rchan-gitlab both might be valid, but completely based on the email leak and not the fact the the list of users is itself available. Sorry I missed that initially.

Ron Chan @rchan-gitlab · 1 year ago — Contributor

Sounds good I'll respect our past decision and keep it consistent with our new reports, thanks for the involvement @ngeorge1 @dcouture !

Edited by Ron Chan 1 year ago

Please register or sign in to reply

Ron Chan added severity 4 scoped label and removed priority 3 severity 3 labels 1 year ago

Dan Jensen removed Accepting merge requests label 1 year ago

Dan Jensen added backend label 1 year ago

Dan Jensen added workflow planning breakdown scoped label 1 year ago

Dan Jensen added 1 deleted label 1 year ago

Dan Jensen added Epic 6340 label 1 year ago

Rohit Shambhuni changed the description 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

Michelle Gill added FY22 Q3 scoped label 1 year ago

Pavel Shutsin assigned to @pshutsin 1 year ago

Pavel Shutsin changed milestone to %14.4 1 year ago

Pavel Shutsin added workflow in dev scoped label and automatically removed workflow planning breakdown label 1 year ago

Pavel Shutsin changed weight to **2** 1 year ago

GitLab Bot added estimation completed scoped label and automatically removed estimation needed label 1 year ago

Pavel Shutsin added workflow in review scoped label and automatically removed workflow in dev label 1 year ago

Michelle Gill @m_gill · 1 year ago — Developer

🎉 This went out with the 14.3.1 release!! Great job @pshutsin 🎉

Michelle Gill closed 1 year ago

Costel Maxim mentioned in issue #219914 (closed) 1 year ago

Michael Henriksen @mhenriksen · 1 year ago — Developer

This is fixed in 14.3.1. Closing.

Michael Henriksen @mhenriksen · 1 year ago — Developer

This is fixed in 14.3.1. Closing.

GitLab SecurityBot @gitlab-securitybot · 1 year 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.

Dominic Couture made the issue visible to everyone 1 year ago

Please register or sign in to reply