Closed Issue created 1 year ago by **Harish Ramachandran**

Users can be added to group via API but not UI with LDAP group sync enabled

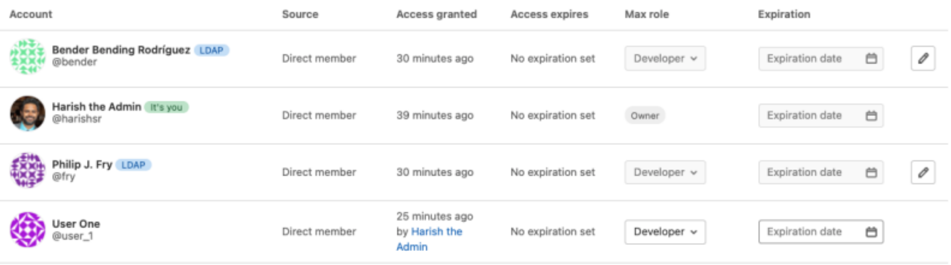
Found in Federal ticket 1420

When LDAP group sync is enabled and a GitLab group has an LDAP group link, then individual users cannot be manually added to the group via the UI.

However, using this API call to add a member to a group, a non-LDAP user *can* be added to the group. Here, I added `@user_1`, who has `id: 32`, to the group:

```
curl --request POST --header "PRIVATE-TOKEN: <token>" \
>      --data "user_id=32&access_level=30" "https://gitlab.local/api/v4/groups/61/members"
{"id":32,"name":"User One","username":"user_1","state":"active","avatar_url":"https://secure.gravata
```

This can be confirmed in the UI, too.



Account	Source	Access granted	Access expires	Max role	Expiration	
Bender Bending Rodríguez LDAP @bender	Direct member	30 minutes ago	No expiration set	Developer ⌄	Expiration date	✎
Harish the Admin It's you @harishsr	Direct member	39 minutes ago	No expiration set	Owner	Expiration date	
Philip J. Fry LDAP @fry	Direct member	30 minutes ago	No expiration set	Developer ⌄	Expiration date	✎
User One @user_1	Direct member	25 minutes ago by Harish the Admin	No expiration set	Developer ⌄	Expiration date	

Afterwards, trying to remove the user from the group using the API yields:

```
curl --request DELETE --header "PRIVATE-TOKEN: <token>" "https://gitlab.local/api/v4/groups/61/membe
{"message":"403 Forbidden"}
```

There also seems to be no way to remove this user from the group now.

This was reproduced in GitLab 14.3.

I've marked this issue as Confidential because of the security implications.

Proposal:

Looks like a missing authorization check on the REST API. Might be worth checking and addressing if there is a corresponding GraphQL endpoint like this as well that is also vulnerable?

We might also have to see why DELETE action is not permitted? It is good that it is not permitted but is that due to having the authorization check in place or due to some other bug?

Edited 7 months ago by Dominic Couture

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

Harish Ramachandran added Support Team Contributions customer ldap security labels 1 year ago

Harish Ramachandran added group authentication and authorization scoped label 1 year ago

GitLab Bot added type bug scoped label 1 year ago

Brad Sevy @brad · 1 year ago Developer

The customer affected is a 110-seat United States Federal Premium customer

Edited by Brad Sevy 1 year ago

GitLab SecurityBot added security-sp-label-missing security-triage-appsec labels 1 year ago

GitLab Bot @gitlab-bot · 1 year ago Maintainer

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

GitLab Bot added devops manage section dev scoped labels 1 year ago

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

Rohit Shambhuni @rshambhuni · 1 year ago Developer

This is a Medium severity issue so adding severity 3 priority 3 labels.

Rohit Shambhuni @rshambhuni · 1 year ago Developer

Given the severity, we have to follow the security MR process on this one.

Orit Golowinski @ogolowinski · 1 year ago Developer

@lmcandrew Is this a regression? If not, it should probably be labeled type feature as (even though not desired) there may be different behavior in UI and API. WDYT?

/cc @hsutor @rshambhuni

Orit Golowinski @ogolowinski · 1 year ago Developer

@hsutor as it doesn't look like someone worked on this in the previous milestone, this should probably move to %14.6

Rohit Shambhuni @rshambhuni · 1 year ago Developer

@ogolowinski I'm not sure if this is a regression but I have seen quite a few variations of vulnerabilities like these in ~"group::access" where the access control/permission checks on the UI don't match with what is happening on the REST/GraphQL API and vice-versa. These types of vulnerabilities fall under a class called Insecure Direct Object Reference (IDOR) vulnerabilities. I'm investigating if we can proactively find IDOR issues like these through tools like Semgrep.

I have added a Proposal section to the issue description with some ideas on how to fix this and potentially other vulnerabilities related to this one.

I think this is a ~vulnerability so type feature may not be relevant here given what I said above.

Please register or sign in to reply

Rohit Shambhuni added severity 3 scoped label 1 year ago

Rohit Shambhuni added Weakness CWE-285 scoped label 1 year ago

Rohit Shambhuni added priority 3 scoped label 1 year ago

Rohit Shambhuni removed security-sp-label-missing label 1 year ago

Rohit Shambhuni removed security-triage-appsec label 1 year ago

GitLab SecurityBot @gitlab-securitybot · 1 year ago Reporter

@hsutor @lmcandrew @dennis @rshambhuni This issue is ready for triage as per HackerOne process.

About this automation: AppSec Escalation Engine

GitLab SecurityBot changed due date to January 04, 2022 1 year ago

Rohit Shambhuni changed due date to January 06, 2022 1 year ago

Rohit Shambhuni changed due date to January 04, 2022 1 year ago

Hannah Sutor changed milestone to %14.5 1 year ago

GitLab Bot added Accepting merge requests label 1 year ago

Liam McAndrew added bug vulnerability scoped label 1 year ago

Rohit Shambhuni changed the description 1 year ago

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

Rohit Shambhuni changed the description 1 year ago

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

GitLab SecurityBot @gitlab-securitybot · 11 months ago 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 %14.6 11 months ago

GitLab SecurityBot @gitlab-securitybot · 10 months ago Reporter

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

About this automation: AppSec Escalation Engine

Hannah Sutor mentioned in issue gitlab-org/manage/general-discussion#17440 (closed) 10 months ago

Hannah Sutor changed milestone to %Backlog 10 months ago

Hannah Sutor @hsutor · 10 months ago Developer

Moving this out of old milestone %14.6 since no work has been done on it

Markus Koller assigned to @toupeira 10 months ago

Markus Koller added workflow in dev scoped label 10 months ago

Markus Koller changed milestone to %14.8 10 months ago

GitLab Bot removed Accepting merge requests label 10 months ago

Hannah Sutor mentioned in issue gitlab-org/manage/general-discussion#17455 (closed) 9 months ago

Michelle Gill added backend label 9 months ago

Hannah Sutor mentioned in issue gitlab-org/manage/general-discussion#17462 (closed) 9 months ago

Markus Koller added workflow in review scoped label and automatically removed workflow in dev label 9 months ago

Markus Koller added workflow awaiting security release scoped label and automatically removed workflow in review label 9 months ago

Andrew Kelly @ankelly · 9 months ago Developer

Closing, this was released in 14.8.2

Andrew Kelly closed 9 months ago

GitLab SecurityBot removed security-issue-escalated label 9 months ago

Cynthia "Arty" Ng removed Support Team Contributions label 8 months ago

Dominic Couture changed the description 7 months ago

Dominic Couture made the issue visible to everyone 7 months ago

Please register or sign in to reply