

ESCALATED: Projects are allowed to add members with different domain email address despite restricting in group settings

[HackerOne report #679567](#) by [ashish_r_padelkar](#) on 2019-08-22, assigned to [gitlab_cmaxim](#) :

Summary

Hello,

In new feature <https://gitlab.com/help/user/group/index#allowed-domain-restriction-premium-only>, it is mentioned that You can restrict access to groups and their underlying projects by allowing only users with email addresses in particular domains to be added to the group

However, this restriction only works at group level and not projects underneath it.

Steps to reproduce

1. Go to group settings at `/-/edit#js-permissions-settings` and put `gitlab.com` under `Restrict membership by email`.
2. Now try to add members at group membership with different email and it wont allow you to do.
3. Now as a maintainer ,go to projects underneath it and add the email with different domain and it will successfully adds the member.

What is the current *bug* behavior?

Allows adding email of different domains at project level despite setting it to group level

What is the expected *correct* behavior?

The settings should be applied at all levels as per documentation.

Output of checks

This bug happens on GitLab.com and probably on omnibus installations too


Regards,
Ashish

Impact


Allows adding members with different domain email addresses at project level despite group level settings.

Edited 3 years ago by [GitLab SecurityBot](#)


📁 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


 [Email domain restrictions apply also to projects](#)


172450


 144  


Activity

 [GitLab SecurityBot](#) added [HackerOne](#) [security](#) labels 3 years ago


 [GitLab SecurityBot](#) added [priority 3](#) [severity 3](#) scoped labels 3 years ago


 [Costel Maxim](#) changed due date to November 26, 2019 3 years ago


 [Costel Maxim](#) added [group authentication and authorization](#) [docs manage](#) scoped labels 3 years ago


 [Costel Maxim @cmaxim](#) 3 years ago
Confirmed ./cc [@jeremy](#) [@lmcandrew](#)


[Developer](#)

 [GitLab SecurityBot](#) added [security-epi-milestone](#) label 3 years ago


 [Liam McAndrew](#) assigned to [@mksionek](#) 3 years ago

 [GitLab SecurityBot](#) removed [security-epi-milestone](#) label 3 years ago


 [Gosia Ksionek](#) mentioned in issue [#7297 \(closed\)](#) 3 years ago


 [Achilleas Pinjellis @axil](#) 3 years ago
Is this a security vulnerability or an implementation "feature"? 🤔
[@jeremy](#), should we prioritize this?
cc'ing [@amandaruada](#) who pointed me to this. This is confusing to customers <https://gitlab.zendesk.com/agent/tickets/135129>


[Maintainer](#)

 [Gosia Ksionek @mksionek](#) 3 years ago
I know, I opened an MR. I spoke to Jeremy about it some time ago.


[Developer](#)

 [GitLab SecurityBot](#) added [security-issue-escalated](#) label 3 years ago


 [GitLab SecurityBot](#) changed title from **Projects are allowed to add members with different domain email address despite restricting in group settings** to **ESCALATED: Projects are allowed to add members with different domain email address despite restricting in group settings** 3 years ago

 [GitLab SecurityBot @gitlab-securitybot](#) 3 years ago
[@jeremy](#) This security issue is overdue.
Please make sure that a new milestone is assigned within 7 business day(s) and provide some context, if possible. Thanks!
More information: [Escalation Engine Workflow](#)


[Author](#) [Reporter](#)

 [GitLab SecurityBot @gitlab-securitybot](#) 2 years ago
[@ebrinkman](#) [@jeremy](#) This security issue is overdue.
Please make sure that a new milestone is assigned within 7 business day(s) and provide some context, if possible. Thanks!
More information: [Escalation Engine Workflow](#)


[Author](#) [Reporter](#)

 [GitLab SecurityBot @gitlab-securitybot](#) 2 years ago
[@ebrinkman](#) [@jeremy](#) This security issue is overdue.
Please make sure that a new milestone is assigned within 7 business day(s) and provide some context, if possible. Thanks!
More information: [Escalation Engine Workflow](#)

[Author](#) [Reporter](#)

 [GitLab SecurityBot @gitlab-securitybot](#) 2 years ago
[@ebrinkman](#) [@jeremy](#) This security issue is overdue.
Please make sure that a new milestone is assigned within 7 business day(s) and provide some context, if possible. Thanks!
More information: [Escalation Engine Workflow](#)

[Author](#) [Reporter](#)

 [Eric Brinkman](#) changed milestone to [%Next 4-7 releases](#) 2 years ago

GitLab Bot

@qitlab-bot · 2 years ago

Setting [Category:Authentication and Authorization](#) based on --"group:access".

Maintain

GitLab Bot

@qitlab-bot · 2 years ago

Setting [Category:Authentication and Authorization](#) based on --"group:access".

Maintain

GitLab Bot

@qitlab-bot · 2 years ago

Setting [Category:Authentication and Authorization](#) based on --"group:access".

Maintain

GitLab Bot

 added [Category:Authentication and Authorization](#) label 2 years ago

GitLab SecurityBot

@qitlab-securitybot · 2 years ago
[@ebcrinkman](#) [@jeremy](#), This security issue is overdue.
Please make sure that a new milestone is assigned within 7 business day(s) and provide some context, if possible. Thanks!
More information: [Escalation Engine Workflow](#)

Author Report

GitLab SecurityBot

@qitlab-securitybot · 2 years ago
[@ebcrinkman](#) [@jeremy](#), This security issue is overdue.
Please make sure that a new milestone is assigned within 7 business day(s) and provide some context, if possible. Thanks!
More information: [Escalation Engine Workflow](#)

Author Report

Costel Maxim

@cmaksim · 2 years ago
This restriction should be applied to all group members (either a user or members of a group added to a group).

Develop

GitLab SecurityBot

@qitlab-securitybot · 2 years ago
[@ebcrinkman](#) [@jeremy](#), This security issue is overdue.
Please make sure that a new milestone is assigned within 7 business day(s) and provide some context, if possible. Thanks!
More information: [Escalation Engine Workflow](#)

Author Report

GitLab SecurityBot

@qitlab-securitybot · 2 years ago
[@ebcrinkman](#) [@jeremy](#), This security issue is overdue.
Please make sure that a new milestone is assigned within 7 business day(s) and provide some context, if possible. Thanks!
More information: [Escalation Engine Workflow](#)

Author Report

GitLab SecurityBot

@qitlab-securitybot · 2 years ago
[@ebcrinkman](#) [@jeremy](#), This security issue is overdue.
Please make sure that a new milestone is assigned within 7 business day(s) and provide some context, if possible. Thanks!
More information: [Escalation Engine Workflow](#)

Author Report

Michelle Gill

@m_oll · 2 years ago
[@cmaksim](#) I have the same question as [this](#). - is this a vulnerability or a feature? It doesn't look like this was intended to apply to projects inherited by the group yet based on this question/answer: #7297 (comment 230072340) and I see that documentation for this feature has been updated to remove the portion about "projects": <https://gitlab.com/help/user/openup/index#allowed-domain-restriction-premium>

Develop

Costel Maxim

 mentioned in issue gitlab-com/gi-security/engineering#926 2 years ago

Costel Maxim

@cmaksim · 2 years ago
[@m_oll](#) It looks like this works as intended. [@mksionek](#) Could we consider this report a feature/improvement and change it to public with P4/S4?

Develop

Gosia Ksionek

@mksionek · 2 years ago
Yes, so sorry I missed that :(

Develop

Costel Maxim

@cmaksim · 2 years ago
I have updated the labels and removed the confidential flag. Thanks

Develop

Please register or sign in to reply

Costel Maxim

 added [category](#) 1 [severity](#) 4 [type](#) feature scoped labels and automatically removed [priority](#) 3 [severity](#) 3 labels 2 years ago

Costel Maxim

 made the issue visible to everyone 2 years ago

GitLab Bot

 added [section](#) dev scoped label 2 years ago

Ron Chan

 added [security-backlog](#) closed scoped label 2 years ago

Dominic Couture

 added [security-backlog](#) reclassified scoped label and automatically removed [security-backlog](#) closed label 2 years ago

Gosia Ksionek

 unassigned [@mksionek](#) 1 year ago

GitLab Bot

 added [Acquivity](#) move requests label 1 year ago

Jamie Reid

@jreid · 1 year ago
[@mushakov](#) A premium SaaS customer with 8500 seats is running into this with some regularity. Despite a fairly restrictive configuration on their namespace, users are able to successfully SAML link accounts with email domains other than that which is permitted in their namespace allowlist, and then get directly added to projects.

At the moment the impact is relatively benign (i.e. bad data and broken reports) but they like the use of an email domain allowlist as a secondary security feature.

It seems, per this issue, that's not being honoured at the project level.

cc: @cmarksle1

Develop

Jamie Reid

@jreid · 1 year ago
In my mind, this should be characterized as a bug or security vulnerability as any reasonable person would interpret a top-level email domain allowlist to apply to all children of the namespace. Subgroups behave this way, but curiously, projects do not.

Develop

Alex Pooley

@aleypooley · 1 year ago
[@jreid](#) [@mushakov](#) I'm a bit unclear on how this feature operates. Is it correct that the domain list can only be defined in the top level group? This seems to be the case in code, but the docs don't mention this? <https://docs.gitlab.com/ee/user/openup/index.html#restrict-group-access-by-domain>

Also, this work is behind a feature flag. Should this still be the case?

Maintain

Jamie Reid

@jreid · 1 year ago
Yes that reflects my experience and understanding. [@aleypooley](#), One can define an email domain allowlist at the top-level namespace only. Subgroups do not offer the ability to define an alternative allowlist.

IMO there is no longer a need for a feature flag since this has been out for some time and enabled on .COM.

Develop

Melissa Ushakov

@mushakov · 1 year ago
[@aleypooley](#), I agree with [@jreid](#) re: feature flag not being needed.
[@lmcandrew](#), I wonder why this didn't come up in the [feature flag review issue](#) 🤔

Develop

Please register or sign in to reply

 Melissa Ushakov changed milestone to [%Next 1-3 releases](#) 1 year ago

Developer

Maintainer

Developer

Developer

 Alex Pooley changed weight to 2 1 year ago

Developer

Developer

Developer

 Orit Golowinski added candidate 14.1 scoped label 1 year ago

Developer

Developer

Please [register](#) or [sign in](#) to reply