

Service desk email address of a project is being leaked through graphql to non-members of the project even if a custom suffix is set for the same.

[HackerOne report #1439254](#) by albatraoz on 2022-01-02, assigned to [@cmaxim](#):

[Report](#) | [Attachments](#) | [How To Reproduce](#)

Report

Summary

I've [reported](#) this vulnerability previously too but closed it as N/A myself as the service desk email address is guessable if we have a project name. But this time I saw some activity on gitlab [issues](#) about the visibility & it has been changed to [reporter](#) & also if any project owner decides to add suffix to their service desk email address to defend the spam, that too would be exposed through graphql.

Steps to reproduce

1. Visit <https://gitlab.com/-/graphql-explorer>
2. Put the following graphql query and hit play

```
query{
  project(fullPath:"gitlab-org/gitlab") {
    id
    serviceDeskAddress
  }
}
```

You will see the internal service desk email of the project in the response.

```
{
  "data": {
    "project": {
      "id": "gid://gitlab/Project/278964",
      "serviceDeskAddress": "contact-project+gitlab-org-gitlab-278964-issue-[@]incoming.gitlab.com"
    }
  }
}
```

What is the current *bug* behavior?

Service desk email address is visible to non members of a project.

What is the expected *correct* behavior?

Service desk email address should be visible only to members of a project with minimum reporter level access.

Relevant logs and/or screenshots



Issue references

[#345692 \(closed\)](#)

[!74179 \(merged\)](#)

Impact reference

[#329446 \(comment 563640175\)](#)

Impact

Even though the service desk email address is guessable If we have the project name, If the owner decides to add a secret suffix only visible & shared with project members, the email address would be leaked to non members through graphql. This can lead to issue spam or vandalism of a project.

Attachments


Warning: Attachments received through HackerOne, please exercise caution!


- [GraphQL.png](#)

How To Reproduce


Please add [reproducibility information](#) to this section:

-
-
-


 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


 [Allow reporters to see the service desk email address](#)

 14.5  


Activity




[GitLab SecurityBot](#) changed due date to March 26, 2022 [10 months ago](#)



[GitLab SecurityBot](#) added [HackerOne](#) [security](#) labels [10 months ago](#)



[GitLab SecurityBot](#) added [Weakness](#) [CWE-284](#) [type bug](#) [priority 3](#) [severity 3](#) scoped labels [10 months ago](#)



[GitLab SecurityBot](#) [@gitlab-securitybot](#) · 10 months ago


Author Reporter

[HackerOne comment](#) by bassguitar :

Thanks for the submission [@]albatraoz,

This looks like the same issue you reported in #1330273. That said, we are closing this report as Duplicate .

Kind regards, [@]bassguitar



[GitLab SecurityBot](#) [@gitlab-securitybot](#) · 10 months ago

Author Reporter

[HackerOne comment](#) by albatraoz :

Heyy [@]bassguitar ,

That report of me was self closed by me thinking that there is no impact(It was not closed as N/A by h1 or gitlab). That's why I opened a new report with the impact as I was not able to reopen the previous report. Can we get this to the [@]gitlab team or [@]gitlab_cmaxim to evaluate the report & the impact please?

Thanks & Regards, [@]albatraoz

[GitLab SecurityBot](#) [@gitlab-securitybot](#) · 10 months ago

Author Reporter



[HackerOne comment](#) by albatraoz :

Any update?



[GitLab SecurityBot](#) @gitlab-securitybot · 10 months ago

Author

Reporter

[HackerOne comment](#) by albatraoz :

The triager thought that the original report of me of which this report is marked as duplicate as closed as N/A by gitlab or h1. But the original report was my report & I closed it by myself because I was not able to prove impact. But now I'm able to prove impact for the same report but I was not able to reopen the previous report so I wrote this new report with the impact. The triager marked this report as duplicate of my own report which is funny. I'd suggest to go through this report once again through an h1 triager or someone from the gitlab team.



[GitLab SecurityBot](#) @gitlab-securitybot · 10 months ago

Author

Reporter

[HackerOne comment](#) by bassguitar :

Hi [@]albatraoz,

Thank you for your report. We appreciate the time and effort spent in putting this report together, however we want to make you aware that Mediation should only be used in cases when all normal discussions with the HackerOne team have been attempted and there has been no satisfactory resolution. More information about Mediation is available [here](#):

Please respect the guidelines above and only request mediation if it's deemed absolutely necessary. We also recommend taking a moment to review the HackerOne Code of Conduct: <https://www.hackerone.com/policies/code-of-conduct>

Kind regards, [@]bassguitar



[GitLab SecurityBot](#) @gitlab-securitybot · 10 months ago

Author

Reporter

[HackerOne comment](#) by albatraoz :

Hey [@]bassguitar ,

I thought once the report gets closed as duplicate the communication doesn't go through properly & that's why opened a mediation request. I will make sure it doesn't happen again. Hope this report gets reevaluated asap.

Thanks & Regards, [@]albatraoz



[Costel Maxim](#) added [group](#) [product planning](#) [devops](#) [plan](#) scoped labels 10 months ago



[Costel Maxim](#) @cmaxim · 10 months ago

Developer

FYI: [@mjwood](#) [@johnhope](#) this is similar to [#342823 \(closed\)](#) just that the email address is leaked via GraphQL.



[John Hope](#) @johnhope · 10 months ago

Developer

I think this should be a relatively straightforward fix so proposing it for [%14.8](#). Thanks [@cmaxim](#).

Edited by [John Hope](#) 10 months ago

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



[GitLab SecurityBot](#) @gitlab-securitybot · 10 months ago

Author

Reporter

[@cdybenko](#) [@johnhope](#) [@donaldcook](#) [@cmaxim](#) This issue is ready for triage as per [HackerOne process](#).

About this automation: [AppSec Escalation Engine](#)




[GitLab Bot](#) added [section](#) [dev](#) scoped label 10 months ago



GitLab Bot @gitlab-bot · 10 months ago

Maintainer

Please add the ~vulnerability label to this issue if appropriate. Regardless, please add a comment or  to indicate you have seen this message.



John Hope mentioned in issue [plan#501 \(closed\)](#), 10 months ago



John Hope added [workflow ready for development](#) scoped label 10 months ago



Marc Shaw assigned to [@marc shaw](#) 10 months ago



Marc Shaw added [workflow in dev](#) scoped label and automatically removed [workflow ready for development](#) label 10 months ago



GitLab Bot added [bug vulnerability](#) scoped label 10 months ago



John Hope @johnhope · 10 months ago

Developer

Thanks for taking this [@marc shaw](#) 🙌

Do you have an MR WIP and an estimate for delivery? If you think it'll be in the [%14.8](#) security release please add that milestone!



Marc Shaw @marc shaw · 10 months ago

Maintainer

Updated the milestone 🎉

MR is hopefully merged tomorrow or day after: https://gitlab.com/gitlab-org/security/gitlab/-/merge_requests/2118



Marc Shaw @marc shaw · 9 months ago

Maintainer

The MR is merged and should be in the latest security release))

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



Marc Shaw changed milestone to [%14.8](#) 10 months ago



Marc Shaw added [workflow awaiting security release](#) scoped label and automatically removed [workflow in dev](#) label 9 months ago



Michelle Gill added [backend](#) label 9 months ago



Costel Maxim @cmaxim · 9 months ago

Developer

Issue fixed. Closing issue.



Costel Maxim closed 9 months ago



Andrew Kelly @ankelly · 9 months ago

Developer

This was assigned CVE-2022-0373



GitLab Bot mentioned in issue [gitlab-org/quality/triage-reports#6366 \(closed\)](#), 9 months ago



GitLab SecurityBot @gitlab-securitybot · 8 months ago

Author

Reporter

[@cmaxim](#) - 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.



Costel Maxim made the issue visible to everyone [8 months ago](#)

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