

## Guest user can see tag names

[HackerOne report #833334](#) by lzzsec on 2020-03-28, assigned to [@rchan-gitlab](#)

[Security Implementation Issue](#)

### Summary

According to <https://gitlab.com/help/user/permissions> "Guest users can access GitLab Releases for downloading assets but are not allowed to download the source code nor see repository information like tags and commits. By querying releases api for a project that user has guest access to they are able to see tag names under the `_links.self` JSON field

### Steps to reproduce

1. Create new private project
2. Add a guest user
3. Go to Home --> Releases <https://gitlab.com/-/releases>
4. Click New Release, enter any tagname and click create tag
5. As guest user go to Releases the api page at [https://gitlab.com/api/v4/projects/<project\\_id>/releases?per\\_page=20](https://gitlab.com/api/v4/projects/<project_id>/releases?per_page=20) will load
6. Check the JSON response and see the tag name under `_links.self`
7. Alternatively query the releases API with guest user token

```
curl -X GET -H "Private-Token: <PRIVATE_TOKEN>" https://gitlab.com/api/v4/projects/<project_id>/releases
```

JSON snippet with `_links.self` and tag name

```
{
  "_links": {
    "self": "https://gitlab.com/<group/>projects/<->/releases/<tag_name>"
  }
}
```

### Impact

Guest users can see tag names

### Examples

This happens on [gitlab.com](https://gitlab.com).

What is the current *bug* behavior?

Guest users can see tag names

What is the expected *correct* behavior?

Tag names should not be displayed to guest users.

### Impact

Guest users can see tag names

Edited 1 year ago by [Shinya Manda](#)

📎 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 📄 2

Relates to

🔗 Know whether release tags exists or not as a guest in private projects

#12145

🕒 Backlog

🔗 A guest user can see Release Tag from Group Release endpoint

#293711

📅 Mar 14, 2021

### Activity

🤖 **GitLab SecurityBot** added [priority 3](#) [severity 3](#) scoped labels [2 years ago](#)

🤖 **GitLab SecurityBot** added [HackerOne](#) [security](#) labels [2 years ago](#)

🗨 **Ron Chan** mentioned in issue [#37325 \(closed\)](#) [2 years ago](#)

📌 **Ron Chan** added 1 deleted label [2 years ago](#)

📌 **Ron Chan** added [discussion release](#) scoped label [2 years ago](#)



**Ron Chan** @rchan-gitlab · [2 years ago](#)

👤 Contributor

Issue confirmed. Guest user can see private project's tag names in the release API endpoint. The tag names are returned in `_links` parameter

Information returned for guest user:

```
{
  "name": "Release-1364097",
  "description": "second tag",
  "description_html": "\u003cp data-sourcepos=\u0026quot;1:1-1:10\u0026quot; dir=\u0026quot;auto\u0026quot;\u003csecond tag\u003c/p\u003e",
  "created_at": "2020-03-29T21:01:01.436Z",
  "released_at": "2020-03-29T21:01:01.436Z",
  "author": {
    "id": "5616676",
    "name": "Ron Chan",
    "username": "rchan-gitlab",
    "state": "active",
    "avatar_url": "https://assets.gitlab-static.net/uploads/-/system/user/avatar/5616676/avatar.png",
    "web_url": "https://gitlab.com/rchan-gitlab",
    "upcoming_release": false,
    "assets": {
      "count": 0,
      "links": []
    },
    "_links": {
      "self": "https://gitlab.com/rchan-gitlab/q7474750/-/releases/v0.0444"
    }
  },
  "name": "Release-1364084",
  "description": "first tag",
  "description_html": "\u003cp data-sourcepos=\u0026quot;1:1-1:9\u0026quot; dir=\u0026quot;auto\u0026quot;\u003cfirst tag\u003c/p\u003e",
  "created_at": "2020-03-29T20:56:28.620Z",
  "released_at": "2020-03-29T20:56:28.616Z",
  "author": {
    "id": "5616676",
    "name": "Ron Chan",
    "username": "rchan-gitlab",
    "state": "active",
    "avatar_url": "https://assets.gitlab-static.net/uploads/-/system/user/avatar/5616676/avatar.png",
    "web_url": "https://gitlab.com/rchan-gitlab",
    "upcoming_release": false,
    "assets": {
      "count": 0,
      "links": []
    },
    "_links": {
      "self": "https://gitlab.com/rchan-gitlab/q7474750/-/releases/v0.01"
    }
  }
}
```

/cc @jmesheil @hampton

Edited by **Ron Chan** [2 years ago](#)



**Jackie Porter** @jporter · [2 years ago](#)

👤 Developer

Thanks I've added the relevant labels to get this triaged through the team



**John Hampton** @jhampton · [2 years ago](#)

Thank you for the ping and details [@rchan-gitlab](#)!

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

📌 **Jackie Porter** added [workflow](#) [planning breakdown](#) [todo](#) [planning](#) [new bug](#) -12671529 scoped labels [2 years ago](#)

📌 **Jackie Porter** added [Category Release Orchestration](#) [needs weight](#) labels [2 years ago](#)

🕒 **Jackie Porter** changed milestone to [%Backlog](#) [2 years ago](#)

📅 **Costel Maxim** changed due date to June 30, 2020 [2 years ago](#)


🤖 **GitLab Bot** added [Accepting merge requests](#) label [2 years ago](#)

📌 **Jackie Porter** removed [Release P2](#) label [2 years ago](#)

🗨 **Jackie Porter** mentioned in issue [#229386 \(closed\)](#) [2 years ago](#)


 Jackie Porter marked this issue as related to [#12145 \(closed\)](#) 2 years ago

 Vladimir Shushlin removed needs weight label 2 years ago

 Vladimir Shushlin changed weight to 1 2 years ago

 Jackie Porter added For Scheduling label 2 years ago

 Jackie Porter added cid active scoped label and automatically removed cid planning label 2 years ago

 Jackie Porter added workflow scheduling scoped label and automatically removed workflow planning breakdown label 2 years ago

 **Jackie Porter** added low hanging fruit label and removed For Scheduling label 2 years ago


 **GitLab Bot** added `section ops` scoped label 2 years ago

 Jackie Porter added Release P1 scoped label 2 years ago

 Jackie Porter added `workflow` `ready for development` scoped label and automatically removed `workflow` `scheduling` label 2 years ago

 **Dominic Couture** added `security-backlog` `valid` scoped label 2 years ago


 Jackie Porter added `group` `release` scoped label 2 years ago

 Jackie Porter removed 1 deleted label 2 years ago


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

 **GitLab SecurityBot** added `Weakness CWE-657` scoped label and automatically removed `Weakness CWE-284` label 2 years ago

 **GitLab SecurityBot** added [Weakness CWE-284](#) scoped label and automatically removed [Weakness CWE-657](#) label [2 years ago](#)

 **GitLab SecurityBot** added [Weakness CWE-657](#) scoped label and automatically removed [Weakness CWE-284](#) label [2 years ago](#)

 Andrew Kelly marked this issue as related to [#293711 \(closed\)](#) 2 years ago

 Andrew Kelly mentioned in issue [#293711 \(closed\)](#) 2 years ago

 [Nicole Williams](#) mentioned in issue [gitlab-org/ci-cd/release-group/release#55](#) (closed), 2 years ago

 Nicole Williams assigned to [@shinya.maeda](#) 2 years ago

 Nicole Williams changed milestone to [%13.8](#) 2 years ago

 **GitLab Bot** removed Accepting merge requests label 2 years ago

 Nicole Williams removed Release P1 label 1 year ago

Shinya Maeda@shinyamaeda: 1 year ago


Maintainer

The fix should be


```
diff --git a/lib/api/entities/release.rb b/lib/api/entities/release.rb
index f6c3dd5a589..145813c2998 100c44
--- a/lib/api/entities/release.rb
+++ b/lib/api/entities/release.rb
@@ -33,7 +33,7 @@ class Release < Grape::Entity
   end

   expose :evidences, using: Entities::Releases::Evidence, expose_nil: false, if: ->{ _ } { can_download_code? }
-  expose :links do
+  expose :links, if: ->{ _ } { can_download_code? } do
     expose :self_url, as: :self, expose_nil: false
     expose :edit_url, expose_nil: false
   end
```

Shinya Maeda added [workflow: in dev](#) scoped label and automatically removed [workflow: ready for development](#) label 1 year ago

 **Shinya Maeda** @shinya-maeda · 1 year ago Maintainer


[@nfriend](#) FYI, I created [that issue](#) because we're going to hide `_links` for guests for fixing this vulnerability.

 **Nathan Friend** @nfriend · 1 year ago Contributor

[@shinya-maeda](#) Nice, makes sense to me. This would make the REST API consistent with GraphQL API: [https://gitlab.com/gitlab-org/gitlab/-/blob/778ebcbcd5d147c2c0620c770f3abc5916fcddeb/app/graphql/types/release\\_links\\_type.rb#L17](https://gitlab.com/gitlab-org/gitlab/-/blob/778ebcbcd5d147c2c0620c770f3abc5916fcddeb/app/graphql/types/release_links_type.rb#L17)

If you wanted to take this a step further, you could also only show `edit_url` if the user has `update_release` permissions (see [https://gitlab.com/gitlab-org/gitlab/-/blob/778ebcbcd5d147c2c0620c770f3abc5916fcddeb/app/graphql/types/release\\_links\\_type.rb#L17](https://gitlab.com/gitlab-org/gitlab/-/blob/778ebcbcd5d147c2c0620c770f3abc5916fcddeb/app/graphql/types/release_links_type.rb#L17)). But this isn't a security issue and is unrelated to this change, so feel free to ignore.


For context, the frontend uses the existence of `edit_url` to determine whether or not to show the edit button.

 **Shinya Maeda** @shinya-maeda · 1 year ago Maintainer

[@nfriend](#) Thank you for providing the info. It's burden for us to keep GraphQL and REST API consistent. Maybe we should generalize it in the future if possible.

If you wanted to take this a step further, you could also only show `edit_url` if the user has `update_release` permissions (see [https://gitlab.com/gitlab-org/gitlab/-/blob/778ebcbcd5d147c2c0620c770f3abc5916fcddeb/app/graphql/types/release\\_links\\_type.rb#L17](https://gitlab.com/gitlab-org/gitlab/-/blob/778ebcbcd5d147c2c0620c770f3abc5916fcddeb/app/graphql/types/release_links_type.rb#L17)). But this isn't a security issue and is unrelated to this change, so feel free to ignore.


It seems `edit_url` in REST API is already guarded by `update_release`. Given the permission requires Developer role or above, only `self_url` seems a vulnerability today.

 **Luke Duncalfe** @luke · 1 year ago Maintainer

[@shinya-maeda](#)

It's burden for us to keep GraphQL and REST API consistent. Maybe we should generalize it in the future if possible.

I think in this case, since the `ReleaseLinkType` uses `ReleasePresenter` your change in <https://gitlab.com/gitlab-org/security/gitlab-micropublic-requests/1163> to the presenter will affect both APIs 🚩 (although all fields in `ReleaseLinkType` already need `download_code` due to the type authorization).

 **Shinya Maeda** @shinya-maeda · 1 year ago Maintainer

[@luke](#) Yes, the presenter is shared, but still there are few inconsistencies between REST API's Entity specific auth code and GraphQL specific auth code. Developers could easily miss something when they extend attributes and auth logic in the future.

Maybe we should entirely move the auth logic to the presenter, but not sure if it's possible. Ideally, [we call GraphQL from the REST API](#).

Edited by [Shinya Maeda](#) 1 year ago


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

Shinya Maeda changed the description 1 year ago

Shinya Maeda added [workflow: in review](#) scoped label and automatically removed [workflow: in dev](#) label 1 year ago


Shinya Maeda added [workflow: verification](#) scoped label and automatically removed [workflow: in review](#) label 1 year ago

Dominic Couture added [Weakness: CWE-285](#) scoped label and automatically removed [Weakness: CWE-657](#) label 1 year ago


 **Shinya Maeda** @shinya-maeda · 1 year ago Maintainer

Async Update

- All security MRs are on review

 **Shinya Maeda** @shinya-maeda · 1 year ago Maintainer

- We're waiting for the maintainer to reassign to the security bot for merge

 **Shinya Maeda** @shinya-maeda · 1 year ago Maintainer


- All set. We're waiting for the security release. We can close this issue after that.

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


 **Shinya Maeda** @shinya-maeda · 1 year ago Maintainer

Closing as [the security patch](#) has been released.

Shinya Maeda closed 1 year ago

 **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