Closed · Issue created 2 years ago by GitLab SecurityBot

Stored XSS on PyPi simple API endpoint

HackerOne report #856836 by vakzz on 2020-04-23, assigned to @dcouture:

Summary

The recently released PyPi package feature has a new endpoint at `/api/:version/projects/:id/packages/pypi/simple/*package_name` which exposes an HTML page listing the package versions. The `package_link`'s are generated using the following code:

package_presenter.rb#L50

```
      def package_link(url, required_python, filename)
        "<a href=\"#{url}\" data-requires-python=\"#{required_python}\">#{filename}</a><br>"
      end
```

The only sanitation on `required_python` is that it is less than 50 characters (db constraint), otherwise arbitrary html can be injected.

Steps to reproduce

1. Create project
2. Create a pypi package with `requires_python='"><script>alert(1)</script>'`

```
curl -v "https://token:$TOKEN@gitlab.com/api/v4/projects/18315917/packages/pypi" -F content=@/tmp/lala.txt -F requires_python=2.7 -F version=1 -F name='package_test_1' -F requires_python='">'
```

1. Visit the simple api endpoint and see the injected code: https://gitlab.com/api/v4/projects/18315917/packages/pypi/simple/package_test_1

```
<!DOCTYPE html>
<html>
  <head>
    <title>Links for package_test_1</title>
  </head>
  <body>
    <h1>Links for package_test_1</h1>
    <a href="https://gitlab.com/api/v4/projects/18315917/packages/pypi/files/lala.txt#sha256=" data-requires-pyth
  </body>
</html>
```

Currently will be blocked by the csp on gitlab.com

Impact

- An attacker could execute arbitrary javascript by sending a user or getting them to click on a url to the simple api endpoint

Examples

- https://gitlab.com/api/v4/projects/18315917/packages/pypi/simple/package_test_1

What is the current *bug* behavior?

The user supplied fields used by the `package_presenter` are not all sanitized

What is the expected *correct* behavior?

All of the user supplied fields in `package_presenter` should be sanitized before being turned into html

Output of checks

This bug happens on GitLab.com

Impact

- An attacker could execute arbitrary javascript by sending a user or getting them to click on a url to the simple api endpoint

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 1

Relates to

Stored XSS on the Packages page
#217685 · 13.3 · Jul 27, 2020

Activity

GitLab SecurityBot added HackerOne security labels 2 years ago

GitLab SecurityBot added priority 3 severity 3 scoped labels 2 years ago

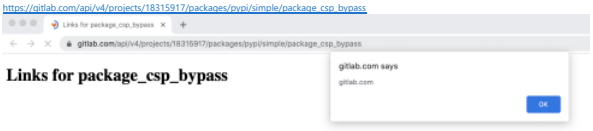
GitLab SecurityBot @gitlab-securitybot · 2 years ago (Author) (Reporter)

HackerOne comment by vakzz :

The CSP bypass from https://hackerone.com/reports/836649#activity-7513032 could be used by breaking up the injection into multiple versions (although it appears to be fixed for newly uploaded files lfs files?)

```
curl -v "https://__token__:$TOKEN@gitlab.com/api/v4/projects/18315917/packages/pypi" -F content=@/tmp/lala.txt -F
curl -v "https://__token__:$TOKEN@gitlab.com/api/v4/projects/18315917/packages/pypi" -F content=@/tmp/lala.txt -F
```

https://gitlab.com/api/v4/projects/18315917/packages/pypi/simple/package_csp_bypass



Attachments

Warning: Attachments received through HackerOne, please exercise caution!

- Screen_Shot_2020-04-23_at_2.48.01_pm.png

Dominic Couture @dcouture · 2 years ago (Developer)

@jhampton @trizzi An XSS was reported to us in the new PyPi package listing API.

John Hampton @jhampton · 2 years ago

Thank you for the ping @dcouture.

Tim Rizzi @trizzi · 2 years ago Developer

Added to the %13.2 milestone which will hit our due date of July 23.

Please register or sign in to reply

Dominic Couture added group package devops package scoped labels 2 years ago

GitLab SecurityBot changed due date to July 23, 2020 2 years ago

GitLab Bot mentioned in issue #215804 (closed) 2 years ago

Tim Rizzi changed milestone to %13.2 2 years ago

GitLab Bot added Accepting merge requests label 2 years ago

GitLab Bot mentioned in issue #216398 (closed) 2 years ago

GitLab Bot mentioned in issue #217258 (closed) 2 years ago

GitLab Bot mentioned in issue #218177 (closed) 2 years ago

GitLab Bot mentioned in issue #218919 (closed) 2 years ago

Giorgenes Gelatti changed weight to **2** 2 years ago

Giorgenes Gelatti assigned to @ggelatti 2 years ago

Giorgenes Gelatti @ggelatti · 2 years ago Contributor

Async Issue Update

Status

- **Complete:** `50%`
- **Confidence:** `50%`

Notes

I've investigated a solution and I'm working on figuring out the exact format of the field for validation.

Giorgenes Gelatti added workflow in dev scoped label 2 years ago

GitLab Bot removed Accepting merge requests label 2 years ago

Giorgenes Gelatti @ggelatti · 2 years ago Contributor

Async Issue Update

Status

- **Complete:** `90%`
- **Confidence:** `90%`

Notes

I've pushed a fix MR.

Merge Requests

https://qitlab.com/qitlab-org/security/qitlab/-/merge_requests/555 - `100% done, 90% confident, in review`

Giorgenes Gelatti added workflow in review scoped label and automatically removed workflow in dev label 2 years ago

GitLab Bot mentioned in issue #219673 (closed) 2 years ago

Tim Rizzi mentioned in issue #217685 (closed) 2 years ago

Tim Rizzi marked #217685 (closed) as a duplicate of this issue 2 years ago

Tim Rizzi marked this issue as related to #217685 (closed) 2 years ago

GitLab Bot mentioned in issue #220706 (closed) 2 years ago

Tim Rizzi mentioned in issue #220240 (closed) 2 years ago

GitLab Bot mentioned in issue #222207 (closed) 2 years ago

GitLab Bot mentioned in issue #223626 (closed) 2 years ago

GitLab Bot mentioned in issue #225107 (closed) 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.

Dominic Couture made the issue visible to everyone 2 years ago

GitLab SecurityBot @gitlab-securitybot · 2 years ago Author Reporter

HackerOne report #856836 was disclosed on 2020-09-09 @ 21:57.

- Bounty awarded: $3000

Please register or sign in to reply