Dos by Exploiting math feature on issue page.

HackerOne report #1350793 by cancerz on 2021-09-24, assigned to GitLab Team:

Report | Attachments | How To Reproduce

Report

Exploiting markdown with math feature supplying large value result with dos on issue page.

Summary:

the markdown documentation available on docs.gitlab.com

```
Math
View this topic in GitLab.

Math written in LaTeX syntax is rendered with KaTeX.

Math written between dollar signs $ is rendered inline with the text. Math written in a code block w.

This math is inline $`a^2+b^2=c^2`$.

This is on a separate line:

```math
a^2+b^2=c^2
```

I was trying the dos attack with basic math with this payload:

$$a^{2} + b^{2} = c^{2} + a^{2} + b^{2} = c^{2} + a^{2} + b^{2} = c^{2}$$
 and more than 1000 character.

but nothing impactfull, just error rendering alert.

than i see the math feature is support with inline text by suppling us dollar \$ on fron and end \$ not just code block,

Steps To Reproduce:

in my testing i use two accounts, first accounts : administrator page

second accont: attacker.

- 1. The administrator create project with visibility public. than create issue page,
- 2. on attacker tab, open the link issue that was created by first accounts. than comment with normal character to test that the page is fine.
  - than send comments with large math payloads. (the payload is available on this attachment). after succesfully send comments, reload the page as an attacker.. (if attack succesfully the attacker can't click any button, just stuck on loading)
- 3. The administrator open the issue page, reload the browser tab, as an administrator same as attacker can't access everything on issue page, just see the page loading continously.

#### Impact:

issue page can not opened by any other users.

The dministrator issues can't access option to delete, or edit issue, all option are not accesible, just delete the project to make the issue deleted.

supporting materials:

 $[{\hbox{\scriptsize DOS.ISSUE.PAGE.mp4}}]\ videos\ for\ proof-of-concept$ 

[dos.txt] payloads for attack. just copying the payload than paste it on comments and send comments.

This bug happens on GitLab.com

thanks best regards.

#### Impact

issue page can not opened by any other users.

The dministrator issues can't access option to delete, or edit issue, all option are not accesible, just delete the project to make the issue clear.

## Attachments

Warning: Attachments received through HackerOne, please exercise caution!

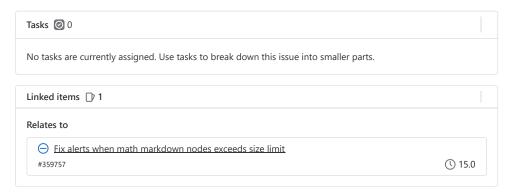
## **How To Reproduce**

Please add <u>reproducibility information</u> to this section:

- 1.
- 2.
- 3.

Edited 8 months ago by Costel Maxim

1 Drag your designs here or click to upload.



## **Activity**





<u>GitLab SecurityBot</u> @gitlab-securitybot · 1 year ago





**<u>HackerOne comment</u>** by cancerz:

after more research, the comments feature on gitlab is available on different places, for example on commits page, i was attack the commits page by comments with the same payloads, after comments send succesfully, the commit page can't accesible, by hacker or by administrator can't edit the commit page again. because the page is stuck.

for example , this is my commits page affected by this attack.. <a href="https://gitlab.com/cancerz/dostest/-/commit/befe31e8509f92cfc4f060590978eb69b1b22720">https://gitlab.com/cancerz/dostest/-/commit/befe31e8509f92cfc4f060590978eb69b1b22720</a>

i think this attack affected on all places on gitlab.com with support comments, or all other places supported markdown,,

## **Attachments**

Warning: Attachments received through HackerOne, please exercise caution!

DOS.COMMIT.mp4



GitLab SecurityBot @gitlab-securitybot · 1 year ago



Reporter

HackerOne comment by bassguitar:

Hi [@]cancerz - I'm discussing this submission internally with the GitLab team. You will be updated as soon as there is additional information to share. Thanks for your patience!



<u>GitLab SecurityBot</u> @gitlab-securitybot · 1 year ago

Author

Reporter

**<u>HackerOne comment</u>** by cancerz:

Hello [@]bassguitar

Thanks for reviewing this report. on this report, I write my account link. but right now my account is blocked. and obviously I can't access my gitlab account anymore. do you know why this happened?

Thanks Regards.

## **Attachments**

Warning: Attachments received through HackerOne, please exercise caution!

- Screenshot 20210927-072509.png
- Screenshot 20210927-072932.png



GitLab SecurityBot @gitlab-securitybot · 1 year ago



( Reporter

**HackerOne comment** by cancerz:

hello [@]dcouture

can you follow up this report.? sorry about my mistake on my other attack report, I hope you can forgive my mistakes. i know i'm wrong. seriously, i'm sorry about that..

thanks regards



GitLab SecurityBot @gitlab-securitybot · 1 year ago



Reporter

**<u>HackerOne comment</u>** by vdesousa:

Hello [@]cancerz,

We are following up on your report. Please don't ping people as it has unnecessary noise on our side. We are currently reviewing it. Thanks.

Regards, Vitor GitLab Security Team



(type bug) scoped label 1 year ago



Vitor Meireles De Sousa @vdesousa · 1 year ago

Developer

Hello @arturoherrero, @brianglanz

We just received this hackerone report on a DoS using a math function in an issue comment. I'm not 100% sure it's for ecosystem/integrations, so let me know if that's not the case 🙂

/cc @mhenriksen as the SC.



Arturo Herrero @arturoherrero · 1 year ago

Maintainer

I think this belongs to group project management, what do you think @jlear?



Jake Lear @jlear · 1 year ago



Yeah, that makes sense. Thanks @arturoherrero

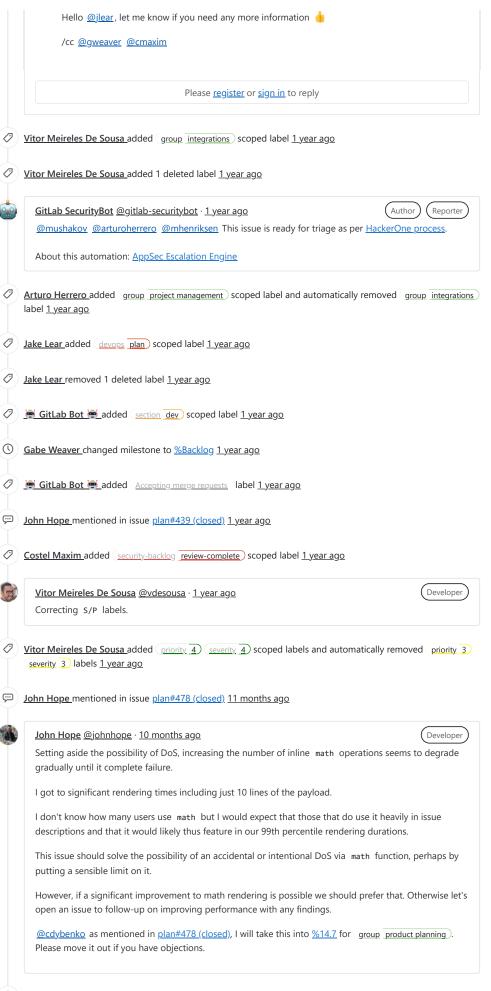


 $\underline{\textbf{Vitor Meireles De Sousa}} \ \underline{\textbf{@vdesousa}} \cdot \underline{\textbf{1 year ago}}$ 

Developer

Thanks @arturoherrero





John Hope added backend label 10 months ago John Hope added workflow ready for development group product planning scoped labels and automatically removed (group project management) label 10 months ago 8 Felipe Artur assigned to @felipe artur 10 months ago Pelipe Artur added workflow in dev scoped label and automatically removed workflow ready for development label 10 months ago (2) GitLab Bot removed Accepting merge requests label 10 months ago Felipe Artur @felipe artur · 10 months ago Maintainer

I opened https://gitlab.com/gitlab-org/security/gitlab/-/merge\_requests/2088 to put a 50 limit of how many math nodes can be rendered, but this is the minimal fix to prevent the request to fail. I think we need to open a couple follow-ups to improve UX and prevent similar problems with other markdown tags.

- Frontend is rendering one alert per math node when <a href="https://gitlab.com/gitlab-">https://gitlab.com/gitlab-</a> org/qitlab/-/blob/master/app/assets/javascripts/behaviors/markdown/render\_math.js. We could probably nest more nodes under an alert or just show one. Screenshot of what is happening below:
- We have a <u>limit of 1MB of size for notes</u>. The <u>sample attachment</u> from this issue to reproduce the problem has ~900KB, but after markdown is rendered it becomes ~4.5MB of HTML saved on note\_html field, which is a bit massive for a single comment. We could consider to also add limit to note html field.

## cc @johnhope



## John Hope @johnhope · 10 months ago

( Developer

@felipe artur I think the 50 limit will go a long way to helping this problem. We could restrict it further without impacting users too much I think. I don't know how many use cases need >20 math nodes in one description/comment. The user can always break it up into multiple comments if necessary.

On the other hand, rendering grows with the number of nodes. Encouraging fewer might have an impact on global average Banzai rendering times?

So 50 is good for the security fix but a follow-up to reduce nodes further would also reduce the cached size without having to limit the note\_html field.

Edited by John Hope 10 months ago



## Felipe Artur @felipe artur · 9 months ago

Maintainer

So 50 is good for the security fix but a follow-up to reduce nodes further would also reduce the cached size without having to limit the note\_html field.

Makes sense. I will create follow-ups from this thread after the security release happens.

Please register or sign in to reply

[ Felipe Artur added workflow in review] scoped label and automatically removed workflow in dev label 10 months ago



## Felipe Artur @felipe artur · 10 months ago

Maintainer

This is not going to make into the next security release, there is no time to create backports, for more information check https://gitlab.com/gitlab-org/security/gitlab/-/issues/578#note 805966856.

@johnhope feel free to move it to the next milestone if you like.

