

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:

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

but nothing impactfull, just error rendering alert.

than i see the `math` feature is support with inline text by supplying 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 acctont : 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 continuously.

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:

[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 administrator issues can't access option to delete, or edit issue, all options are not accessible, just delete the project to make the issue clear.

## Attachments


**Warning:** Attachments received through HackerOne, please exercise caution!

## How To Reproduce

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

- 1.
- 2.
- 3.

Edited 8 months ago by [Costel Maxim](#)

 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

 [Fix alerts when math markdown nodes exceeds size limit](#)  
#359757

 15.0

## Activity

 [GitLab SecurityBot](#) changed due date to December 27, 2021 [1 year ago](#)

 [GitLab SecurityBot](#) added [HackerOne](#) [security](#) labels [1 year ago](#)

 [GitLab SecurityBot](#) added [Weakness](#) [CWE-400](#) [priority 3](#) [severity 3](#) scoped labels [1 year ago](#)



[GitLab SecurityBot](#) @gitlab-securitybot · [1 year ago](#)

Author

Reporter

[HackerOne comment](#) by cancerz :

sorry I forgot to give the link, this is my issue page. i can't open my issue page, waiting the loading more than 30 minutes is not loaded too. just make my machine overloaded.

<https://gitlab.com/cancerz/dos/-/issues/2>



[GitLab SecurityBot](#) @gitlab-securitybot · [1 year ago](#)

Author

Reporter

[HackerOne comment](#) 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 successfully, the commit page can't be accessed, 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.. <https://gitlab.com/cancerz/dos-test/-/commit/befe31e8509f92cfc4f060590978eb69b1b22720>

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

Author

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!



**GitLab SecurityBot** @gitlab-securitybot · 1 year ago

Author

Reporter

[HackerOne comment](#) 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

Author

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

Author

Reporter

[HackerOne comment](#) 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



**GitLab Bot** added `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

Contributor

Yeah, that makes sense. Thanks [@arturoherrero](#)



**Vitor Meireles De Sousa** @vdesousa · 1 year ago

Developer


Thanks [@arturoherrero](#) 😊

Hello @jlear, let me know if you need any more information 🙌

/cc @gweaver @cmaxim

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

 **Vitor Meireles De Sousa** added group `integrations` scoped label `1_year_ago`

 **Vitor Meireles De Sousa** added 1 deleted label `1_year_ago`



**GitLab SecurityBot** @gitlab-securitybot · 1 year ago

Author

Reporter

@mushakov @arturoherrero @mhennriksen This issue is ready for triage as per [HackerOne process](#).


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

 **Arturo Herrero** added group `project management` scoped label and automatically removed group `integrations` label `1_year_ago`


 **Jake Lear** added `devops` `plan` scoped label `1_year_ago`

 **Jake Lear** removed 1 deleted label `1_year_ago`

 **GitLab Bot** added `section` `dev` scoped label `1_year_ago`

 **Gabe Weaver** changed milestone to `%Backlog` `1_year_ago`

 **GitLab Bot** added `Accepting merge requests` label `1_year_ago`

 **John Hope** mentioned in issue [plan#439 \(closed\)](#), `1_year_ago`

 **Costel Maxim** added `security-backlog` `review-complete` scoped label `1_year_ago`




**Vitor Meireles De Sousa** @vdesousa · 1 year ago

Developer

Correcting S/P labels.

 **Vitor Meireles De Sousa** added `priority` `4` `severity` `4` scoped labels and automatically removed `priority` `3` `severity` `3` labels `1_year_ago`

 **John Hope** mentioned in issue [plan#478 \(closed\)](#), `11 months ago`



**John Hope** @johnhope · 10 months ago

Developer

Setting aside the possibility of DoS, increasing the number of inline `math` operations seems to degrade gradually until it complete failure.

I got to significant rendering times including just 10 lines of the payload.

I don't know how many users use `math` but I would expect that those that do use it heavily in issue descriptions and that it would likely thus feature in our 99th percentile rendering durations.


This issue should solve the possibility of an accidental or intentional DoS via `math` function, perhaps by putting a sensible limit on it.


However, if a significant improvement to `math` rendering is possible we should prefer that. Otherwise let's open an issue to follow-up on improving performance with any findings.


@cdybenko as mentioned in [plan#478 \(closed\)](#), I will take this into `%14.7` for `product planning`. Please move it out if you have objections.



 **John Hope** changed milestone to `%14.7` `10 months ago`

 **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

 **Felipe Artur** assigned to [@felipe artur](#) 10 months ago

 **Felipe Artur** added `workflow in dev` scoped label and automatically removed `workflow ready for development` label 10 months ago

  **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](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 [https://gitlab.com/gitlab-org/gitlab/-/blob/master/app/assets/javascripts/behaviors/markdown/render\\_math.js](https://gitlab.com/gitlab-org/gitlab/-/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 [limit of 1MB of size for notes](#). The [sample attachment](#) 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](https://gitlab.com/gitlab-org/security/gitlab/-/issues/578#note_805966856).

[@johnhope](#) feel free to move it to the next milestone if you like.



 **GitLab Bot** mentioned in issue [gitlab-org/quality/triage-reports#6013 \(closed\)](#) 10 months ago



**Costel Maxim** @cmaxim · 10 months ago

Developer

CVE requested: <https://gitlab.com/gitlab-org/cves/-/issues/337>



**GitLab Bot** added `bug` `vulnerability` scoped label 10 months ago



**Felipe Artur** added `workflow` `verification` scoped label and automatically removed `workflow` `in review` label 9 months ago



**Andrew Kelly** @ankelly · 9 months ago

Developer

Closing, this was fixed in 14.8.2



**Andrew Kelly** 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** changed the description 8 months ago ·



**Costel Maxim** @cmaxim · 8 months ago

Developer

Removed `keep confidential` flag. Related with <https://gitlab.com/gitlab-org/release/tasks/-/issues/3520>



**Costel Maxim** made the issue visible to everyone 8 months ago



**Felipe Artur** marked this issue as related to [#359757 \(closed\)](#) 7 months ago



**Felipe Artur** mentioned in issue [#359757 \(closed\)](#) 7 months ago

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