

SSRF possible due to shared address space not being blocked.

[HackerOne report #579934](#) by no1zy on 2019-05-14, assigned to estrike :

Summary

Because `/lib/gitlab/url_blocker.rb` does not block shared address space, [SSRF](#) is possible.

Steps to reproduce

1. Go to `http://{host}/projects/new`.
2. Click to "Repo by URL".
3. Enter the following in Git repository URL field. `http://100.64.0.5:9999/ssrf`
4. Enter other required fields.
5. Click to "Create project".

```
GET /ssrf/info/refs?service=git-upload-pack HTTP/1.1
Host: 100.64.0.5:9999
User-Agent: git/2.18.1
Accept: */*
Accept-Encoding: deflate, gzip
Pragma: no-cache
```

6. If you want to send parameters, specify the URL as follows:

```
http://100.64.0.5:9999/ssrf?param=true#
```

```
GET /ssrf?param=true HTTP/1.1
Host: 100.64.0.5:9999
User-Agent: git/2.18.1
Accept: */*
Accept-Encoding: deflate, gzip
Pragma: no-cache
```

Impact

The shared address space is used as a private network address by the ISP.


Reference: https://en.wikipedia.org/wiki/IPv4_shared_address_space

This issue affects all actions using `/lib/gitlab/url_blocker.rb`.

Proposal

To fix this issue, also block the `100.64.0.0/10` netmask.

Edited 1 year ago by [Sean Carroll](#)

 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](#)



GitLab SecurityBot @gitlab-securitybot · [3 years ago](#)

Author Reporter

[HackerOne comment](#) by [estrike](#) :

Hi @no1zy ,

Thank you for the report. I wanted to request more information on impact. Since this address space is primarily used by ISPs for internal routing between their equipment and a customers, what impact will this have on an installation not in that network?

Best Regards, Ethan Security Team | GitLab Inc.



GitLab SecurityBot @gitlab-securitybot · [3 years ago](#)

Author Reporter

[HackerOne comment](#) by [no1zy](#) :

Hi [@estrike](#),

This has an impact if your ISP has installed gitlab in such an address space. It also has an impact if the ISP is routed to the shared address space from the network where user installed gitlab. If SSRF is possible in the shared address space, it is possible to send malicious requests to the web console of the network device installed in the network. This is affected by the environment where the ISP has shared address space.

Thanks.



Ethan Strike added [priority: 4](#) [severity: 4](#) scoped labels [3 years ago](#)



Ethan Strike added [security request](#) label [3 years ago](#)



Ethan Strike @estrike · [3 years ago](#)

Developer

Overall, the immediate impact is not evident, when this address space is used as intended. Also, this address space is not intended for services. With that said, it does not hurt to add it as part of the local networks that are only allowed if `Allow local networks` is checked.

It would be interesting to hear how this might impact any service provider customers that we do have.

Edited by [Ethan Strike](#) [3 years ago](#)



Ethan Strike added [internal customer](#) label [3 years ago](#)



Stan Hu @stanhu · [3 years ago](#)

Owner

Which ISP actually uses this address space?



Ethan Strike @estrike · [3 years ago](#)

Developer

I do not know, truthfully. I have been unable to find definitive documentation of a particular service provider using it, but I have seen comments about it being used on unidentified residential service providers in US.



GitLab SecurityBot added [security-group-missing](#) [security-triage-appsec](#) labels [3 years ago](#)



GitLab SecurityBot removed [security-triage-appsec](#) label [3 years ago](#)



GitLab SecurityBot added [security-triage-appsec](#) label [3 years ago](#)



Ethan Strike added [group](#) [source code](#) [devops](#) [create](#) scoped labels [3 years ago](#)



GitLab SecurityBot removed [security-group-missing](#) [security-triage-appsec](#) labels [3 years ago](#)



 **GitLab Bot**  added [Accepting merge requests](#) label [3 years ago](#)



R my Coutable removed [Accepting merge requests](#) label [3 years ago](#)



James Ramsay (ex-GitLab) @jramsay-gitlab · 3 years ago

Contributor

@estrike this isn't specific to gitlab-ce#10309854 since it impacts every GitLab URL. Given the large backlog of security issues already on the plate of gitlab-ce#10309854 I'd prefer this issue found a different home 😊 /cc @DouweM



Douwe Maan @DouweM · 3 years ago

Contributor

@estrike A more appropriate team to take this one may be gitlab-ce#10046105 in gitlab-ce#4116705!

/cc @lmcandrew

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



GitLab Bot moved from gitlab-ce#63058 3 years ago



Michelle Gill added [backend](#) label 2 years ago



Michelle Gill changed milestone to [%13.0](#) 2 years ago



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



Michelle Gill removed milestone 2 years ago



Michelle Gill changed milestone to [%13.3](#) 2 years ago



Michelle Gill changed milestone to [%Backlog](#) 2 years ago



GitLab Bot added [section](#) [dev](#) scoped label 2 years ago



Kaung Htet Aung added [security-backlog](#) [risk-acceptance](#) scoped label 2 years ago



GitLab Bot @gitlab-bot · 2 years ago

Maintainer

Setting label(s) [Category:Source Code Management](#) based on group [source code](#).



GitLab Bot added [Category:Source Code Management](#) label 2 years ago



Sean Carroll changed milestone to [%14.4](#) 1 year ago



Sean Carroll changed milestone to [%14.5](#) 1 year ago



Sean Carroll @sean_carroll · 1 year ago

Developer

Moving to [%14.5](#)



James Ritchey removed [security-backlog](#) [risk-acceptance](#) label 1 year ago



Costel Maxim added [security-backlog](#) [review-complete](#) scoped label 1 year ago



Sean Carroll changed the description 1 year ago ·



Sean Carroll @sean_carroll · 1 year ago

Developer

@cmaxim @stanhu

For this issue are we looking to block [100.64.0.0/10](#), or can it be closed with [wontfix](#) ?

To fix this issue, also block the [100.64.0.0/10](#) netmask.



Stan Hu @stanhu · 1 year ago

(Owner)

I'd say let's add 100.64.0.0/10 to the block list, given it's in https://en.wikipedia.org/wiki/Reserved_IP_addresses.



Sean Carroll @sean_carroll · 1 year ago

Developer

Sure thing, thanks [@stanhu](#)

SSOT updated.

Edited by [Sean Carroll](#) 1 year ago

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



[Sean Carroll](#) changed the description 1 year ago ·



[Sean Carroll](#) added to epic [87128](#) 1 year ago



[Sean Carroll](#) mentioned in epic [87128](#) 1 year ago



[Sean Carroll](#) added [Engineering Allocation](#) label 1 year ago



GitLab Bot @gitlab-bot · 1 year ago

Maintainer

👋 @sean_carroll, please ensure the following labels are present for [Engineering Allocation](#) :

- An ~Eng-Consumer::* label
- An ~Eng-Producer::* label
- A ~priority::* label
- A ~severity::* label when the type is ~"bug"



[Sean Carroll](#) changed milestone to [%14.6](#) 1 year ago



Sean Carroll @sean_carroll · 1 year ago

Developer

[@vyaklushin](#) could you please weight this issue.



Vasiliy Iakliushin @vyaklushin · 1 year ago

Maintainer

[@sean_carroll](#) I'd say it's has weight 2.

Note to myself

A similar implementation: https://gitlab.com/gitlab-org/gitlab/blob/479190d8127756043e2cf0637992af298a7b940f/lib/gitlab/url_blocker.rb#L243

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



[Sean Carroll](#) assigned to [@vyaklushin](#) 1 year ago



GitLab Bot removed [Accepting merge requests](#) label 1 year ago



[Vasiliy Iakliushin](#) changed weight to **2** 1 year ago



[James Ritchey](#) added [type: bug](#) scoped label 11 months ago




Sean Carroll @sean_carroll · 11 months ago

Developer


Assigning to [@igor.drozdo](#) as a [%14.7](#) Deliverable.




[Sean Carroll](#) changed milestone to [%14.7](#) 11 months ago

 **Sean Carroll** assigned to [@igor.drozdov](#) 11 months ago

 **Sean Carroll** unassigned [@vyaklushin](#) 11 months ago


 **Sean Carroll** added [workflow](#) [ready for development](#) scoped label 11 months ago


 **Sean Carroll** [@sean_carroll](#) · 11 months ago Developer
[@igor.drozdov](#) this is assigned to you as a [%14.7](#) Deliverable

 **Sean Carroll** added [Deliverable](#) label 11 months ago

 **Igor Drozdov** added [workflow](#) [in review](#) scoped label and automatically removed [workflow](#) [ready for development](#) label 10 months ago

 **GitLab Bot**  mentioned in issue [gitlab-org/quality/triage-reports#6014](#) 10 months ago

 **Igor Drozdov** [@igor.drozdov](#) · 10 months ago Maintainer
[@sean_carroll](#) the MR has been already reviewed by a [backend](#) reviewer and is waiting for AppSec review. Since the next Security Release is at the end of Jan: <https://gitlab.com/gitlab-org/gitlab/-/issues/350093>, I think we're fine here and don't need to take this issue into account on 14.8 scheduling 🙌

 **Sean Carroll** [@sean_carroll](#) · 10 months ago Developer
Perfect. Thank you for the update [@igor.drozdov](#)

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


 **Costel Maxim** [@cmaxim](#) · 10 months ago Developer
CVE requested: <https://gitlab.com/gitlab-org/cves/-/issues/336>


 **Sean Carroll** added [Eng-Consumer](#) [Security](#) [Eng-Producer](#) [Development](#) scoped labels 10 months ago

 **GitLab Bot**  added [bug](#) [vulnerability](#) scoped label 10 months ago


 **Igor Drozdov** changed milestone to [%14.8](#) 10 months ago

 **Igor Drozdov** closed 9 months ago

 **Sean Carroll** [@sean_carroll](#) · 9 months ago Developer
Great to see this closed 🎉


 **Andrew Kelly** [@ankelly](#) · 9 months ago Developer
This was assigned CVE-2022-0249

 **GitLab Bot**  mentioned in issue [gitlab-org/quality/triage-reports#6369](#) 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** [@cmaxim](#) · 8 months ago Developer

Removed the [keep confidential](#) flag.

 **Costel Maxim** made the issue visible to everyone [8 months ago](#)



Caleb Hansard [@caleb.hansard](#) · [7 months ago](#)

Blocking 100.64.0.0/10 has prevented us from using that CIDR block in our EKS clusters. GitLab cannot be deployed to AWS VPCs that utilize that range.

<https://aws.amazon.com/about-aws/whats-new/2018/10/amazon-eks-now-supports-additional-vpc-cidr-blocks/>



Caleb Hansard [@caleb.hansard](#) · [7 months ago](#)

It looks like the original intent of this issue was to prevent the SSRF vulnerability associated with adding a repo by URL. I believe that vulnerability could have enabled access to any internal IP, not just the 100.64.0.0/10 range.

Seeing as 100.64.0.0/10 is used to extend the private IP space that can be used in AWS, I do not think GitLab should block it. If an admin does have a need to block that range, that should be controlled using local firewall rules.

Please remove this block so GitLab can be deployed to AWS VPCs that utilize 100.64.0.0/10.



Caleb Hansard mentioned in issue [#361092 \(closed\)](#) [6 months ago](#)



Caleb Hansard [@caleb.hansard](#) · [6 months ago](#)

[@igor.drozdv](#) [@sean.carroll](#) Please review the comment and issue above. We are unable to utilize the 100.64.0.0/10 range in AWS due to this change.



Sean Carroll [@sean.carroll](#) · [5 months ago](#)

Developer

[@caleb.hansard](#) this issue has been closed. Could you please open a new issue and ping myself and [@igor.drozdv](#) if the problem continues?



Caleb Hansard [@caleb.hansard](#) · [5 months ago](#)

Done. I pinged you in [#361092 \(closed\)](#).

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

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