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, <u>SSRF</u> 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.

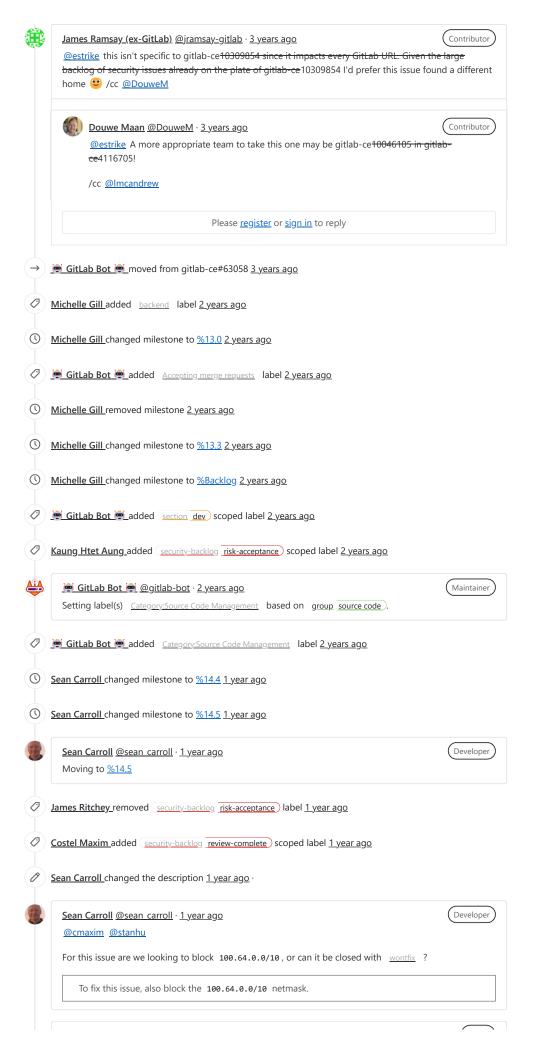
Proposal

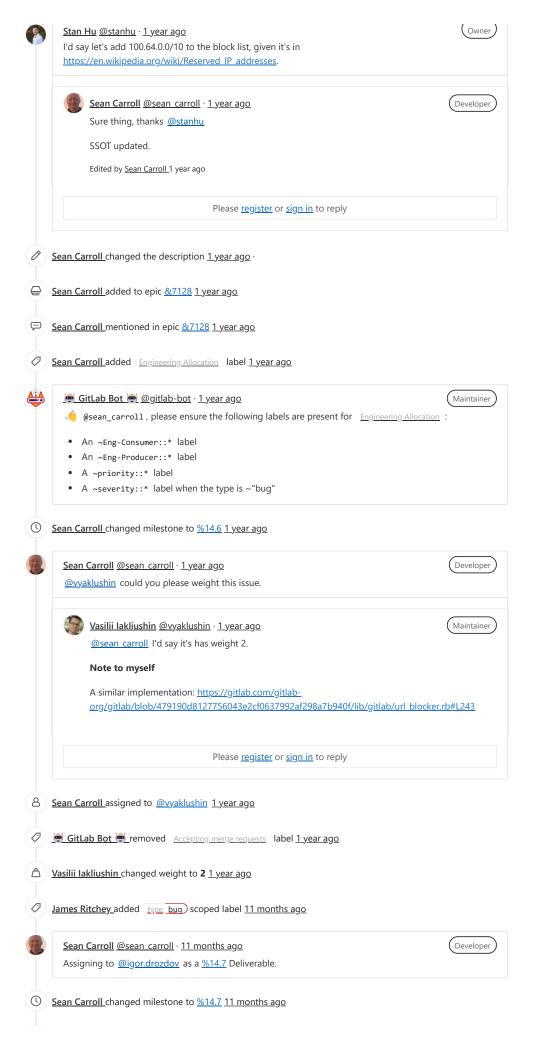
To fix this issue, also block the 100.64.0.0/10 netmask.

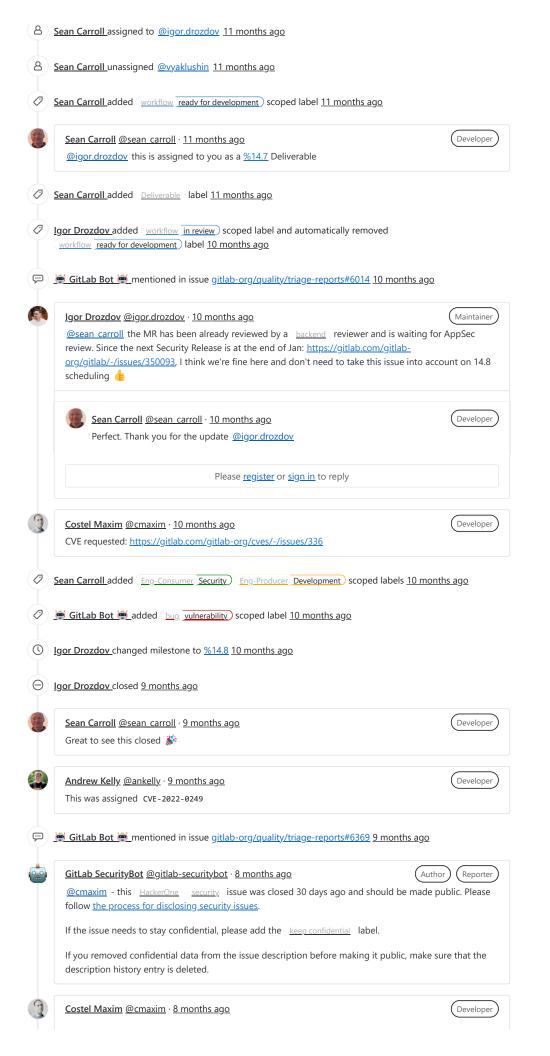
Edited 1 year ago by Sean Carroll

↑ Drag your designs here or click to upload.









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-cidrblocks/



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.drozdov @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.drozdov if the problem continues?



Caleb Hansard @caleb.hansard · 5 months ago

Done. I pinged you in #361092 (closed).

Please <u>register</u> or <u>sign in</u> to reply

Please <u>register</u> or <u>sign in</u> to reply