FULL read SSRF in gogs/gogs

0

✓ Valid Reported on Apr 6th 2022

Description

there is two bypass method for previous fixes of SSRF in gogs
The first is to utilize SSRF attack with a DNS rebinding feature.
The second is to use redirection to a localhost URL.

Proof of Concept

1- go to the webhooks section and create a gogs webhook.
2- enter an URL that redirects to `http://169.254.169.254/metadata/v1.json`
3- test the webhook and see its response; you can read the complete response data from internal resources.
for proof, I get the digitalocean public key `"ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIIaWqg1t4RKxx+G9JUq7rDbpFq/331m7Bei3NVwDBP0r"` there is no security issue within the digitalocean droplet's metadata, but in AWS, GCP, and some other clouds, the access keys can be accessed through this vulnerability.
The account\webhook address that I used through my tests is `https://try.gogs.io/amammad/Azadig/settings/hooks/523`

fix suggestion

`IsLocalHostname` should return the valid IP addresses (of the hostname)

Impact

Any internal resources that have HTTP API and users can access them without credentials are exposed to high-impact danger.

CVE
CVE-2022-1285
(Published)

Chat with us

Vulnerability Type
CWE-918: Server-Side Request Forgery (SSRF)

Severity

High (8.3)

Registry
Golang

Affected Version
*

Visibility
Public

Status
Fixed

Found by

amammad
@amammad
pro

This report was seen 1,130 times.

We are processing your report and will contact the **gogs** team within 24 hours. 8 months ago

amammad modified the report 8 months ago

We have contacted a member of the **gogs** team and are waiting to hear back 8 months ago

Joe Chen validated this vulnerability 8 months ago

amammad has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

amammad 8 months ago Researcher

Hey Joe Chen, I couldn't find out what versions were affected, is it matter for y
affected version precisely?

Chat with us

And also, would you validate the occurrences if they are correct?

And also, would you validate the occurrences if they are correct?

We have sent a fix follow up to the **gogs** team. We will try again in 7 days. 7 months ago

We have sent a second fix follow up to the **gogs** team. We will try again in 10 days. 7 months ago

We have sent a third and final fix follow up to the **gogs** team. This report is now considered stale. 7 months ago

Joe Chen 7 months ago Maintainer

Hey @amammad, I think all versions are affected.

Regarding the occurrences, I think returning IP from `isLocalHostname` doesn't really help for mitigating this vulnerability (i.e. requesting to an IP can still end up in redirection). Thus, I agree disallow redirection in repo migrate and webhook make sense as the fix.

Besides, I can't seem to produce the vulnerability on my DO droplet anymore. The endpoint provided by the docs (https://docs.digitalocean.com/products/droplets/how-to/retrieve-droplet-metadata/) only accepts HEAD and GET requests, but webhooks are POST requests, could you help here? Thanks!

amammad 7 months ago Researcher

Hey Joe, with 308 Status code, The request method, and the body will not be altered, so if you use `308` then a POST request will be sent to the target endpoint.
Differentially, the attacker can send a GET with 301 request because this status code will change any HTTP request to a GET request.

Can you please explain more about this `i.e., requesting to an IP can still end up in redirection` ?

This is my fault, I should say that the main problem with this vulnerability is not an SSRF, the main problem is the TOCTOU vulnerability.
you validate an URL and its IP address when you want to store it for the first time, but when you want to send a request next time to webhook you make another DNS query, and here is the problem, you shouldn't send another DNS query, you should use the validated IP address as the destination, here is the standard procedure for resolving the TOCTOU + SSRF issues that I saw before in many repositories, If you have another better way please inform me whenever you reach it.

Joe Chen 7 months ago Maintainer

Hey @amammad, thanks for a quick response!

[...], with 308 Status code, The request method, and the body will not be altered, so if you use 308 then a POST request will be sent to the target endpoint.

Differentially, the attacker can send a GET with 301 request because this status code will change any HTTP request to a GET request.

TIL!

Can you please explain more about thisi.e., requesting to an IP can still end up in redirection?

Even if the IP is returned and stored, making a request to a remote IP does not guarantee it won't a redirection to different IP in the future, does it? I think the part I'm unclear about this mitigation is that how is retuning the initially resolved IP address help mitigate this problem.

This is my fault, I should say that the main problem with this vulnerability is not an SSRF, the main problem is the TOCTOU vulnerability.
you validate an URL and its IP address when you want to store it for the first time, but when you want to send a request next time to webhook you make another DNS query, and here is the problem, you shouldn't send another DNS query, you should use the validated IP address as the destination, here is the standard procedure for resolving the TOCTOU + SSRF issues that I saw before in many repositories, If you have another better way please inform me whenever you reach it.

I think the solution I'm going with is the combination of a) disallow redirection in repo migrate and webhook b) do `isLocalHostname` validation before every time of use, because I do not think it makes sense to "lock in" IP address for webhooks, which would be a very uncomfortable UX for the product (webhook suddenly failed because I use CDN for the receiving end and the edge nodes changed their IPs). What's your thoughts?

Joe Chen 7 months ago Maintainer

... the rendering is really broken compare to GitHub... It does not display "quotes" correctly...

amammad 7 months ago Researcher

Yeah, your welcome.

For CDN problems, every time you want to send a req to a webhook, you shou
save new IP too.

Actually, in my opinion, there is no need for validating the webhook URL in the first step when you get it from the user because a webhook's IP will be changed each time, whether it will be resolved to a public IP by CDN or a private IP by an attacker (as you said it before)

So we should get the webhook URL and do `IsLocalHostname` each time and return the IP address plus previous return values.

Also, we should send only one DNS query each time and not Two, this is a rule for whatever we should do to fix this issue.

yah seems not the same with GH, so we can use `backquotes.`

Joe Chen 7 months ago Maintainer

OK, I get the part that why `IsLocalHostname` needs to return its resolved IP, and seems we have alignment on doing the validation at every time of use.

Two remaining questions (gosh also no lists?):

A. By "store the IP address" you mentioned previously, did you mean return the resolved IP from `IsLocalHostname` is all we need, or do we need actually store the IP address in the database (for example)? I don't think the latter is worth it since we will validation every time.

B. Could clarify on what "two DNS queries" means? Is it the webhook should directly sending the request to the resolved IP (after getting it from the `IsLocalHostname`)?

amammad 7 months ago Researcher

Sorry for my delay!
about A
You are correct. The first one is what I mean, and storing IP is not a good option.

about B
again You are correct.

Joe Chen 7 months ago Maintainer

Awesome! Thanks for the confirmation.

I'll start working on the patch as soon as my bandwidth permits.

amammad 6 months ago Researcher

Hey Joe, I think you should upgrade your bandwidth :)

Joe Chen 6 months ago Maintainer

I'm currently capped at 24 hours a day, how do I get more xD

Joe Chen marked this as fixed in **0.12.8** with commit **7885f4** 6 months ago

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ✗

Joe Chen 6 months ago Maintainer

A new patch release including the fix to this vulnerability has been published. One thing to note though, after some back and forth, I decided to not return resolved IP address from `IsLocalHostname` because making a request to an IP without a hostname doesn't work for CDN or any floating IP service that relies on the domain name for a correct reverse proxying.

I also think the double DNS queries is fine since most of time DNS queries are cached.

Joe Chen 6 months ago Maintainer

Thanks again for the report!

> Sign in to join this conversation

Chat with us

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us