huntr

Server-Side Request Forgery (SSRF) in gogs/gogs

1

✓ Valid Reported on Jul 17th 2021

✍️ Description

In 2018, this issue was created to address a SSRF vulnerability in gogs wherein an attacker could have gogs send requests to network-internal hosts - a patch for this was released (see diff) and no queries about the SSRF issue seem to have been raised again since (from what I can tell). The patch that was released is a blacklist-based one, this isn't a bad idea in all cases but in this particular case; the blacklist does not cover all resolutions of localhost in quite a few scenarios. The vulnerable code is as follows:

```
var localHostnames = []string{
    "localhost",
    "127.0.0.1",
    "::1",
    "0:0:0:0:0:0:0:1",
}
```

As it does not account for the fact that `127.*.*.*` resolves to localhost too.

🕵️ Proof of Concept

Navigate to `https://try.gogs.io/repo/migrate`.
Under 'clone address' enter `http://127.1.33.7:3306/`.
Fill in the rest of the text areas and proceed.
If the repository was created, port 3306 was open (MySQL) and if not, it was closed. (an error in this case would be `Migration failed: clone: exit status 128 - fatal: unable to access 'http://@127.1.33.7:[closed_port]/': Failed connect to 127.1.33.7:[closed_port]; Connection refused`).

💥 Impact

This vulnerability is capable of allowing attackers to conduct internal port scans.

(please note that the SSRF shown here is a 'blind ssrf' and attackers, from what I can tell, would not gain any sensitive information outside of the open/closed status of a given port).

Occurrences

webhook.go L121-L136

```
var localHostnames = []string{
    "localhost",
    "127.0.0.1",
    "::1",
    "0:0:0:0:0:0:0:1",
}

// isLocalHostname returns true if given hostname is a known local addr
func isLocalHostname(hostname string) bool {
    for _, local := range localHostnames {
        if hostname == local {
            return true
        }
    }
    return false
}
```

CVE
CVE-2022-0870
(Published)

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

Severity
Medium (5)

Affected Version
*

Visibility

Public

Status

Fixed

Found by

Michael Rowley

@michaellrowley

pro ⌄

Fixed by

Michael Rowley

@michaellrowley

pro ⌄

This report was seen 763 times.

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

Michael Rowley has invalidated this vulnerability a year ago

The disclosure bounty has been dropped ×

The fix bounty has been dropped ×

Michael Rowley a year ago Researcher

@admin this was invalidated by mistake, could it be reopened?

Jamie Slome a year ago Admin

Re-opened!

Chat with us

Michael Rowley a year ago Researcher

Thanks!

Michael Rowley 10 months ago Researcher

@admin Is there any way that the Gogs maintainer (dummy issue + `security@gogs.io`) could be re-notified as I think something went wrong during the accidental invalidation that might've caused them to not see this (the gogs/gogs repository is pretty active) and the vulnerability is still valid on the current Gogs version?

Jamie Slome 10 months ago Admin

@michaellrowley - of course, I have just re-sent an e-mail to the maintainers but got a hard bounce when sending it.

It might be worth just sending them a personal e-mail with the URL for the report, as they will be able to gain access once they have signed up.

Let me know if you have any issues with this! ♥

Michael Rowley 10 months ago Researcher

That's strange - I'll try sending them an email like you suggest and see if I can get the link to them.

Michael Rowley 10 months ago Researcher

Putting this here for issue-tracking: https://github.com/gogs/gogs/issues/6754

Michael Rowley modified the report 10 months ago

Michael Rowley modified the report 10 months ago

Joe Chen validated this vulnerability 9 months ago

Michael Rowley has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

Chat with us

Michael Rowley submitted a patch 9 months ago

Michael Rowley 9 months ago

Researcher

Hi, thanks for getting this validated - I've opened a pull request (#6812) that should fix this but I've never written code in Go before so there may be some errors in my style, syntax, or logic that needs fixing although I have tested this Gist so I'm fairly confident in the implementation details.

Joe Chen 9 months ago

Maintainer

Please wait until the "Confirm Fix" button at which point a patch release has been made for users to upgrade. Just FYI that I plan to patch another issue https://github.com/gogs/gogs/issues/6810 together so might need to wait for a bit longer.

Michael Rowley 9 months ago

Researcher

No problem, if there's anything I can do to help with the #6810 patch let me know!

We have sent a fix follow up to the **gogs** team. We will try again in 7 days. 9 months ago

Joe Chen marked this as fixed in **0.12.5** with commit **91f2cd** 9 months ago

Michael Rowley has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

webhook.go#L121-L136 has been validated ✓

Sign in to join this conversation

Chat with us