Sign in

topotam / PetitPotam Public

Notifications Fork 285 Star 1.8k

Code Issues Pull requests 2 Actions Projects Security Insights

main Go to file Code

- PetitPotam
- PetitPotam.exe
- PetitPotam.py
- PetitPotam.sln
- README.md

README

PetitPotam

PoC tool to coerce Windows hosts to authenticate to other machines via MS-EFSRPC EfsRpcOpenFileRaw or other functions :)

The tools use the LSARPC named pipe with inteface c681d488-d850-11d0-8c52-00c04fd90f7e because it's more prevalent. But it's possible to trigger with the EFSRPC named pipe and interface df1941c5-fe89-4e79-bf10-463657acf44d. It doesn't need credentials against Domain Controller :D

About

PoC tool to coerce Windows hosts to authenticate to other machines via MS-EFSRPC EfsRpcOpenFileRaw or other functions.

Readme

Activity

1.8k stars

27 watching

285 forks

Report repository

Releases

No releases published

Packages

No packages published

Contributors 8

Disabling the EFS service seems not to mitigate the "feature"

The Python one require Impacket to be installed, the Windows PoC was done on VS 2019 Community. If compilation problem, remember to add Rpcrt4.lib in the linker. Compile in x86.

Inspired by the previous work on MS-RPRN from @tifkin_ & @elad_shamir and others SpecterOps guys.

Incomplete patch from Microsoft :) https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36942

MS-EFSRPC - Encrypting File System Remote (EFSRPC) Protocol https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-efsr/08796ba8-01c8-4872-9221-1000ec2eff31

Languages

● C 84.1%	● Python 12.6%
● C++ 3.3%	