zcgonvh / EfsPotato Public

master Go to file Code

zcgonvh csc compatibility 0474c9f · last year 10 Commits

EfsPotato.cs	csc compatibility	last year
README.md	Update README.md	3 years ago
test.png	init	3 years ago

README

Exploit for EfsPotato(MS-EFSR EfsRpcEncryptFileSrv with SeImpersonatePrivilege local privalege escalation vulnerability).

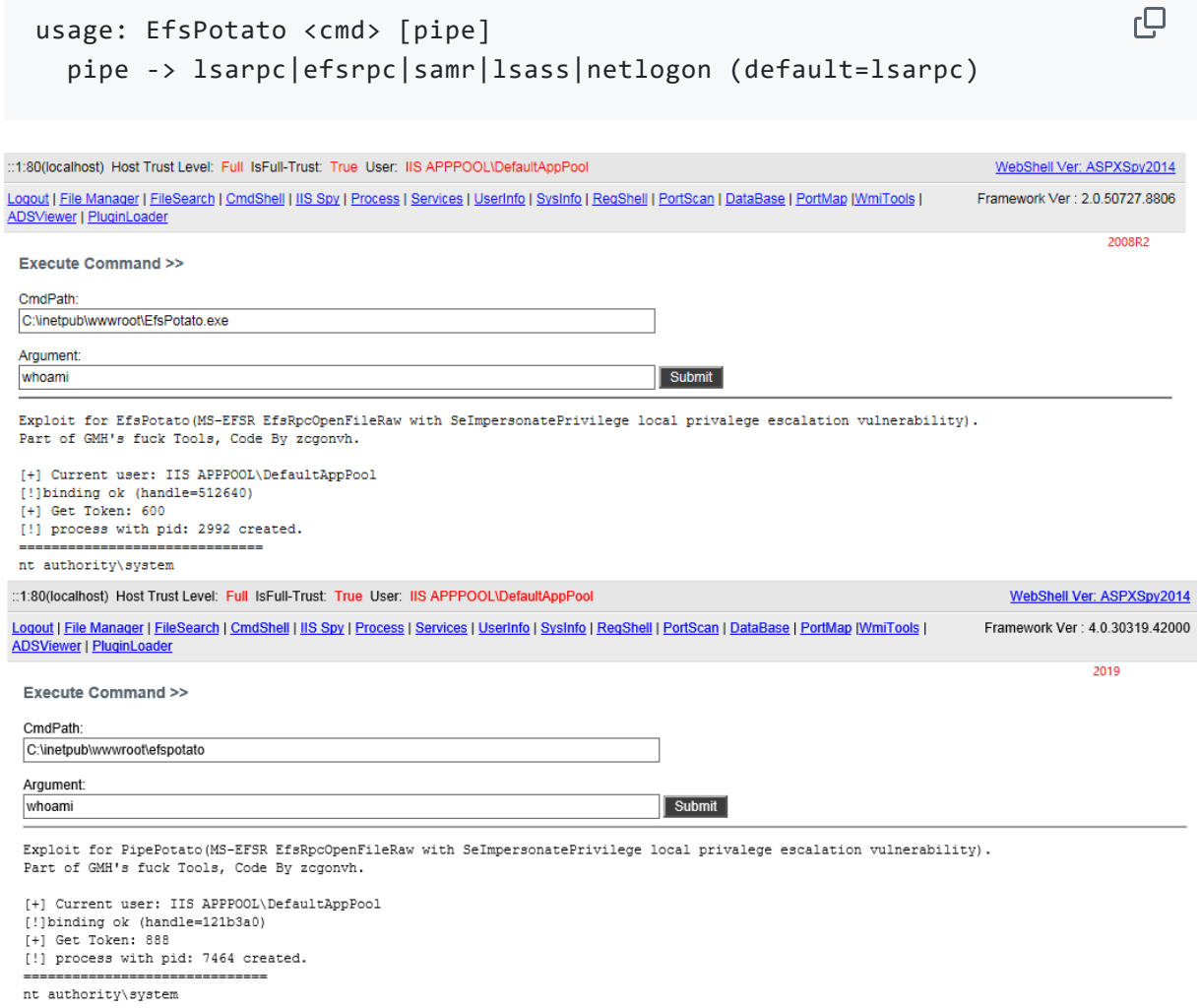
build

```
#for 4.x
csc.exe EfsPotato.cs -nowarn:1691,618
csc /platform:x86 EfsPotato.cs -nowarn:1691,618

#for 2.0/3.5
C:\Windows\Microsoft.Net\Framework\V3.5\csc.exe EfsPotato.cs -nowarn
C:\Windows\Microsoft.Net\Framework\V3.5\csc.exe /platform:x86 EfsPot
```

usage

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



About

Exploit for EfsPotato(MS-EFSR EfsRpcOpenFileRaw with SeImpersonatePrivilege local privalege escalation vulnerability).

Readme
Activity
722 stars
9 watching
120 forks
Report repository

Releases

No releases published

Packages

No packages published

Contributors 3

zcgonvh zcgonvh
xassiz Pablo
BeichenDream beichen

Languages

C# 100.0%