





# /Wsreset.exe

☆ Star

7,060

UAC bypass

Used to reset Windows Store settings according to its manifest file

**Paths:**

C:\Windows\System32\wsreset.exe

**Resources:**

- <https://www.activecyber.us/activelabs/windows-uac-bypass>
- <https://twitter.com/ihack4falafel/status/1106644790114947073>
- <https://github.com/hfiref0x/UACME/blob/master/README.md>

**Acknowledgements:**

- Hashim Jawad ([@ihack4falafel](#))

**Detections:**

- Sigma: [proc\\_creation\\_win\\_uac\\_bypass\\_wsreset\\_integrity\\_level.yml](#)
- Sigma: [proc\\_creation\\_win\\_uac\\_bypass\\_wsreset.yml](#)
- Sigma: [registry\\_event\\_bypass\\_via\\_wsreset.yml](#)
- Splunk: [wsreset\\_uac\\_bypass.yml](#)
- IOC: wsreset.exe launching child process other than mmc.exe
- IOC: Creation or modification of the registry value HKCU\Software\Classes\AppX82a6gwre4fdg3bt635tn5ctqjf8msdd2\Shell\open\command
- IOC: Microsoft Defender Antivirus as Behavior:Win32/UACBypassExp.T!gen

## UAC bypass

During startup, wsreset.exe checks the registry value HKCU\Software\Classes\AppX82a6gwre4fdg3bt635tn5ctqjf8msdd2\Shell\open\command for the command to run. Binary will be executed as a high-integrity process without a UAC prompt being displayed to the user.

wsreset.exe

- Use case:**
- Execute a binary or script as a high-integrity process without a UAC prompt.
- Privileges required:**
- User
- Operating systems:**
- Windows 10, Windows 11
- ATT&CK® technique:**
- [T1548.002: Bypass User Account Control](#)