Wh04m1001 / IDiagnosticProfileUAC Public

Notifications Fork 32 Star 178

Code Issues Pull requests Actions Projects Security Insights

main Go to file Code

Wh04m1001 Update README.md 37c5bef · 2 years ago 3 Commits

| | | |
|---|---|---|
| README.md | Update README.md | 2 years ago |
| main.cpp | Create main.cpp | 2 years ago |

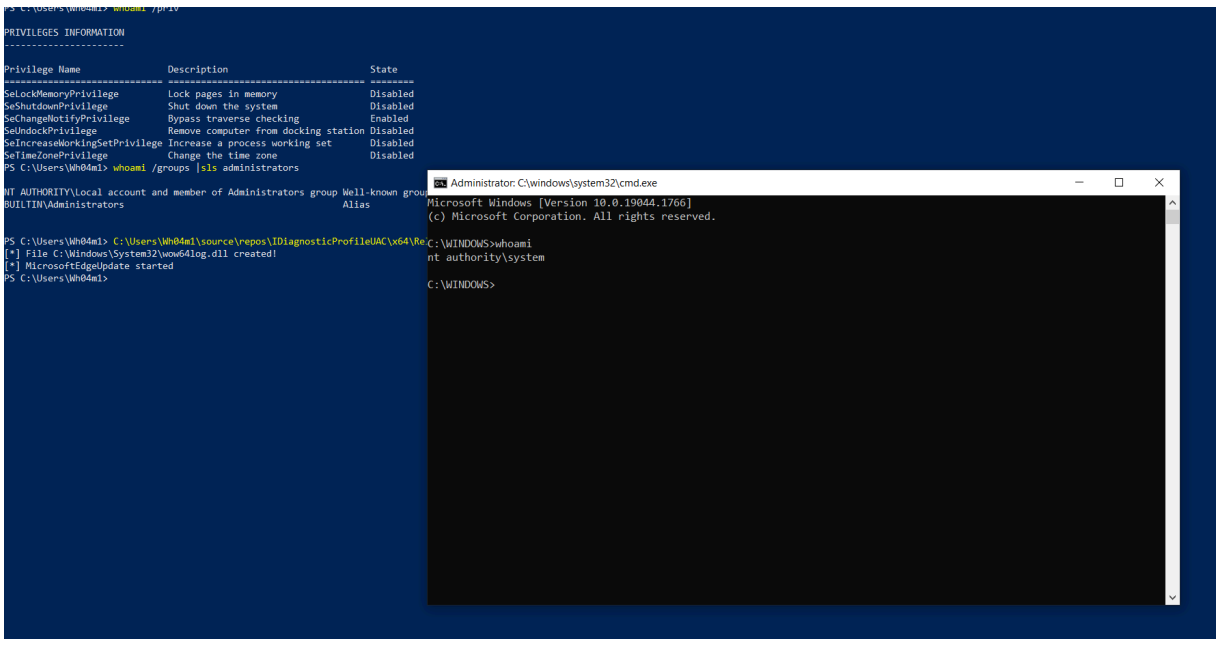
README

# IDiagnosticProfileUAC

Just another UAC bypass using auto-elevated COM object Virtual Factory for DiagCpl (12C21EA7-2EB8-4B55-9249-AC243DA8C666). This COM object can be used to create instance of DiagnosticProfile (D0B7E02C-E1A3-11DC-81FF-001185AE5E76) COM object which exposes SaveDirectoryAsCab method that can be used to move arbitrary file in system32 directory. This PoC copy user specified dll to C:\Windows\System32\wow64log.dll and trigger MicrosoftEdgeUpdate service by creating instance of Microsoft Edge Update Legacy On Demand COM object (A6B716CB-028B-404D-B72C-50E153DD68DA) which run in SYSTEM context and will load wow64log.dll (more info here).

This PoC is inspired by this awesome research from @zcgonvh

http://www.zcgonvh.com/post/Advanced_Windows_Task_Scheduler_Playbook-Part.2_from_COM_to_UAC_bypass_and_get_SYSTEM_dirtectly.html (in chinaese)




## About

*No description, website, or topics provided.*

Readme
Activity
178 stars
7 watching
32 forks
Report repository

## Releases

No releases published

## Packages

No packages published

## Languages

C++ 100.0%