




Privilege escalation (UAC bypass) in ChangePK





Jihad Abdrazak · Follow


3 min read · May 3, 2020

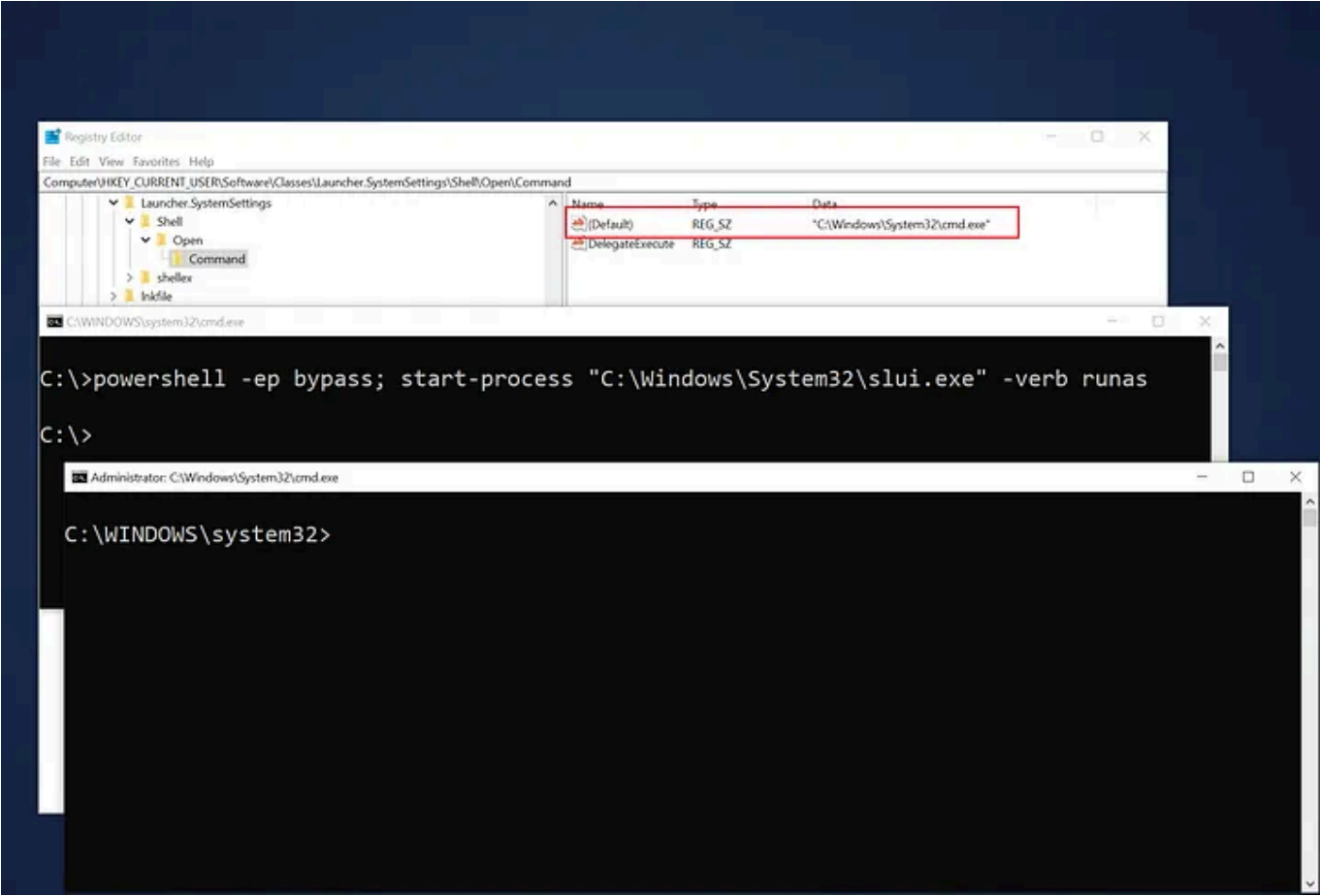
 12











✕

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓ Distraction-free reading. No ads.

✓ Organize your knowledge with lists and highlights.

✓ Tell your story. Find your audience.

Sign up for free

★ Membership

✓ Read member-only stories

✓ Support writers you read most

✓ Earn money for your writing

✓ Listen to audio narrations

✓ Read offline with the Medium app

Try for 5 \$/month

Page 1 of 6

How does Slui UAC bypass work?

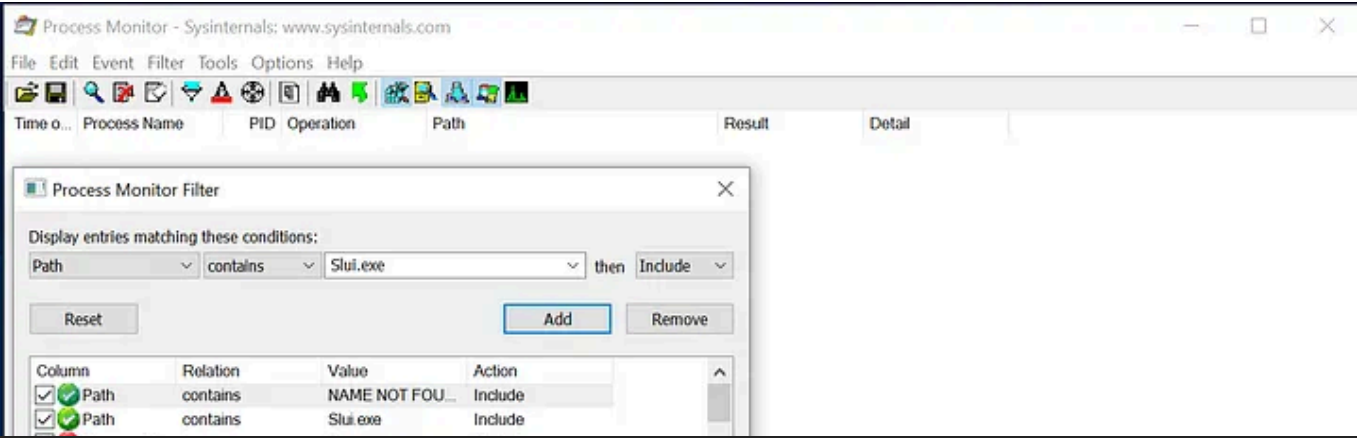
The tool ChangePK is a Windows utility that makes it easy for you and other users to change an old windows activation key to a new one, the tool (ChangePK) doesn't open itself with high privilege but there is another tool opens ChangePK with high privilege named slui.exe. Let's take a look at more details

How does Slui.exe work?

Slui doesn't support a feature that runs it as administrator automatically, but we can do that manually by either clicking on slui with a right click and then click on "Run as administrator" or using this command: powershell.exe start-process slui.exe -verb runas

How did I find the vulnerability?

The tool I used to find the registry key to get a UAC bypass from slui.exe is Procmon. I put some filters in Procmon to find missing registry paths for Slui and I succeed in finding the right missing registry path, let's take a look at it!



Medium

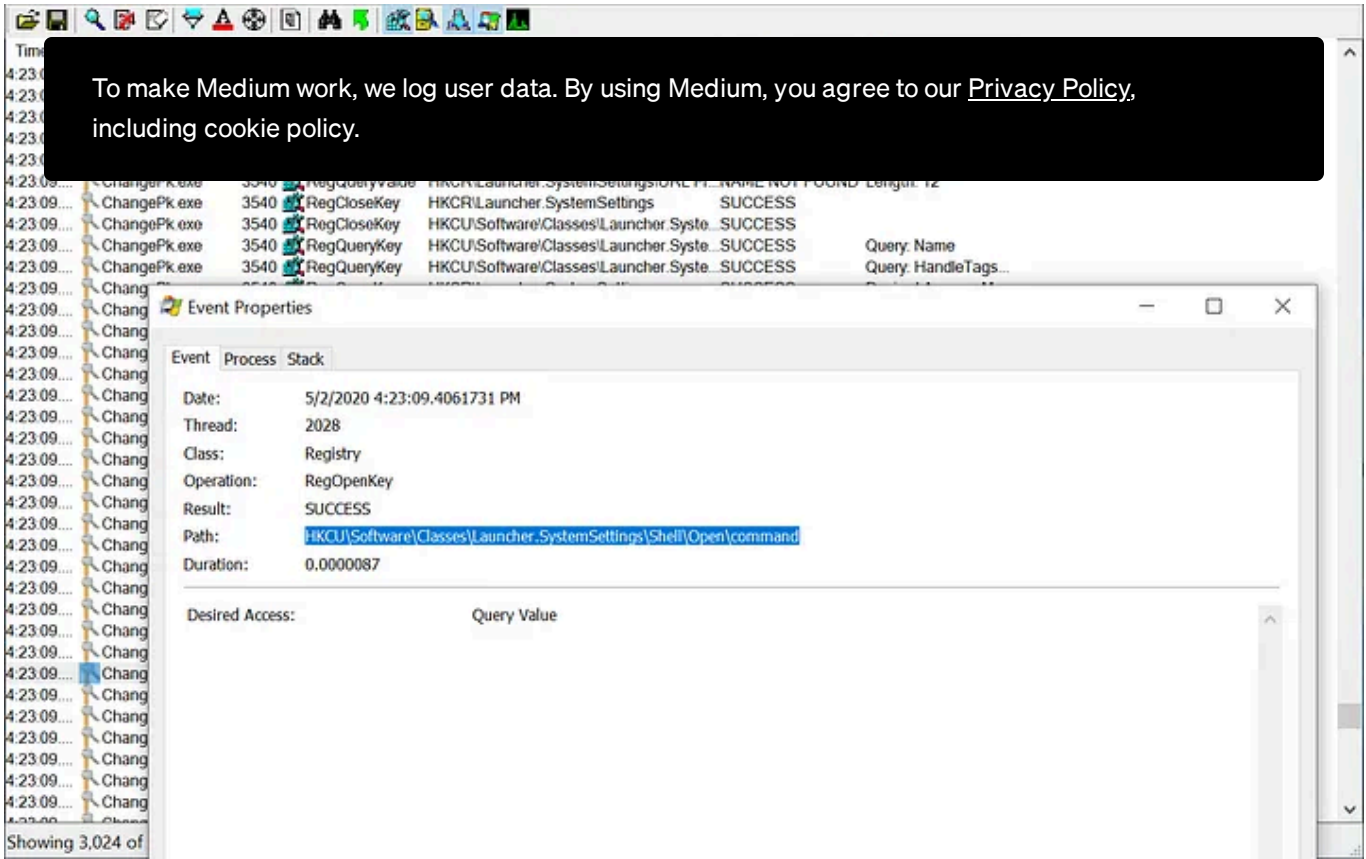
Sign up to discover human stories that deepen your understanding of the world.

Free

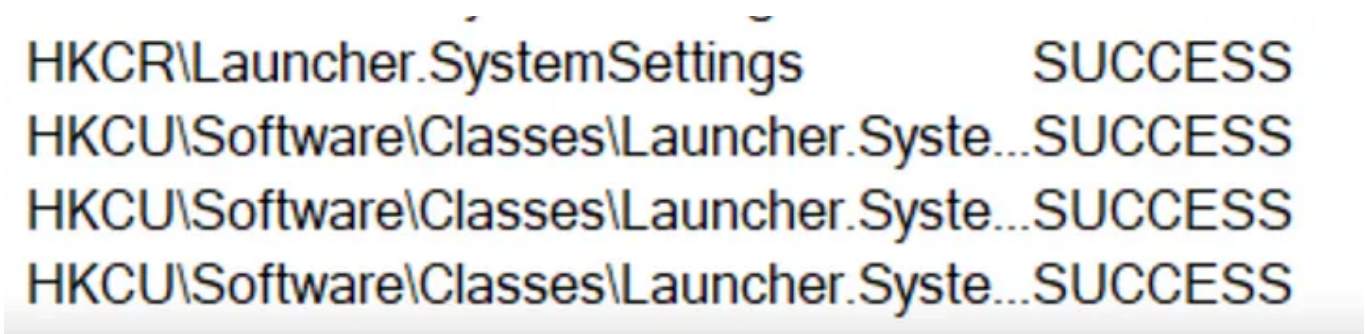
- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

★ Membership

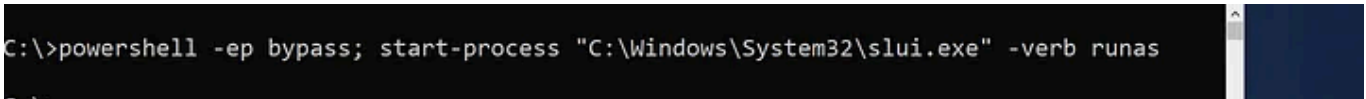
- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app



After creating all the registry paths needed to get a Slui UAC bypass, I got the success word in Procmon, Look at this!



Now It's time to test the bug!



Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

✓

Distraction-free reading. No ads.

✓

Organize your knowledge with lists and highlights.

✓

Tell your story. Find your audience.

★ Membership

✓

Read member-only stories

✓

Support writers you read most

✓

Earn money for your writing

✓

Listen to audio narrations

✓

Read offline with the Medium app

Page 3 of 6

HKCU\Software\Classes\launcher\Systemsettings\Shell\open\command

The

ke

To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy.

The proof of concept:

<https://gist.github.com/homjxi0e/9174952b6535a13a2645978b8abfd541>

Conclusion: Jihad

Research



12



Written by Jihad Abdrazak

Follow



110 Followers

An Ambitious man | Red teamer | Security Researcher | Passionate about windows internals, abusing features and malware analysis

More from Jihad Abdrazak

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

★ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy.

 Jihad Abdrazak

Living off the land (LotL) attack

Introduction Detection evasion’s become the most important part that adversaries focus o...

Jan 16, 2022  4



 Jihad Abdrazak

Living off the land attack

Introduction Detection evasion is considered as the most important part of adversary...

Jan 16, 2022  2



See all from Jihad Abdrazak

Recommended from Medium

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

★ Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app

To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy.

Liwei Zhou

Hack the Box—Walkthrough—Return

Return is an easy machine running the Microsoft Windows operation system. The...

Jun 29 1



tacitPanda

Sau Write-up | Hack The Box

Ok, so this was written almost a year ago! I believe I wrote this up before I even had a...

May 7 1



Satyam Pathania in InfoSec Write-ups

Why I Don’t Recommend People To Get into Cybersecurity?

Cybersecurity isn’t always what it seems—it’s tough, demanding, and stressful.

Oct 24 389 7



AbhirupKonwar in System Weakness

PII Data Breach | Lazy Threat Actor Methodology ☒

Welcome hackers, I am Abhirup Konwar (aka LegionHunter) . In this article I will elaborate...

Oct 24 194 3



Medium

Sign up to discover human stories that deepen your understanding of the world.

Free

- ✓ Distraction-free reading. No ads.
- ✓ Organize your knowledge with lists and highlights.
- ✓ Tell your story. Find your audience.

Membership

- ✓ Read member-only stories
- ✓ Support writers you read most
- ✓ Earn money for your writing
- ✓ Listen to audio narrations
- ✓ Read offline with the Medium app