

Forum: [Hack Forums](#)

Thread: [UAC bypass, bypasses windows defender \(and more\)](#)

moom825 - August 29, 2023, 12:04 pm

Heya all,

I came across this interesting UAC bypass on Twitter. It abuses EventViewer's unsafe deserialization of its RecentViews file (which is publicly accessible). I recreated the entire thing in C# and made improvements. Now, it creates no visible window, is completely automated, and doesn't rely on any external libraries.

After recreating the entire thing, I realized that it was being detected by Windows Defender, not the UAC bypass itself, but the modified RecentViews file. I made some modifications by patching the file before it's written. As of writing this thread, it now successfully bypasses Windows Defender.

I hope you all enjoy it! Feel free to donate by quick hearting. But for those of you who are a bit stingy, here's the link to the GitHub repository: [EventViewer-Unsafe-Deserialization-UACBypass](#)

Enjoy! ?

Skel3r - August 29, 2023, 12:55 pm

Nice work.

You should embed GIF on Github page too :)

moom825 - August 29, 2023, 1:23 pm

(Aug 29, 2023 12:11 PM)m0hx Wrote: [\[CITE\]](#) nice share, i'll give it a try on win11.

seems like its only for 10, it creates the even but didn't do the uac nor anything just exists.
Spoiler [\(Click to View\)](#)

pretty sure can be modified to work.

https://kleenscan.com/scan_result/1844e5daa10a7a59b2560e5528328ab3e864d6123ef28b1b8e23c68d1e4a308f

they did a bunch of updates for windows 11, they could have changed the desearilization method for the recentviews, ill take a look at it when i get home, thx for the heads up

osn64698 - August 30, 2023, 6:25 am

There is no need to try new methods when old ones work perfectly on all OS's with 0 av detection.

<https://www.elastic.co/guide/en/security/current/uac-bypass-via-icmluauil-elevated-com-interface.htm>
!

moom825 - August 30, 2023, 6:06 pm

(Aug 30, 2023 06:25 AM)osn64698 Wrote: [\[CITE\]](#) There is no need to try new methods when old ones work perfectly on all OS's with 0 av detection.

<https://www.elastic.co/guide/en/security/current/uac-bypass-via-icmluautl-elevated-com-interface.html>
|

just tested it, doesn't seem to work on latest version of windows

DramaKing - August 30, 2023, 7:01 pm

(Aug 30, 2023 06:25 AM)osn64698 Wrote: [\[CITE\]](#) There is no need to try new methods when old ones work perfectly on all OS's with 0 av detection.

<https://www.elastic.co/guide/en/security/current/uac-bypass-via-icmluautl-elevated-com-interface.html>
|

The vendor that you linked to is clearly able to detect it.

osn64698 - August 30, 2023, 8:22 pm

(Aug 30, 2023 07:01 PM)DramaKing Wrote: [\[CITE\]](#) The vendor that you linked to is clearly able to detect it.

Nobody detects it, I am saying it from experience. Defender/ Kaspersky/ Bit-Defender/ Avira/ Avast /AVG / Trend Micro etc. I also tested all EDRs.

You don't have to use CoGetObject, people who get detected simply copy and paste the same code, so that is obviously their issue, they should use their 1% brain.

I won't spoon feed HF people since tomorrow you will have 10 new Crypt3rs with UAC Bypass.

MMKS - August 31, 2023, 5:49 am

hello darmaking I need service for fb hack care to help ?

DramaKing - August 31, 2023, 6:04 am

(Aug 31, 2023 05:49 AM)MMKS Wrote: [\[CITE\]](#) hello darmaking I need service for fb hack care to help ?

Misspelling my username, going off-topic, and asking for service in the wrong forum

Anyway, here's a "fb hack:" <https://grahamcluley.com/hack-facebook-sms/>. You can also transfer an associated phone number to your phone.

MMKS - August 31, 2023, 6:32 am

I'm truly sorry for my mistakes... Im in a rush to take down the scammers, can you elaborate how can I use this tool sir ?

DramaKing - August 31, 2023, 7:42 am

(Aug 31, 2023 06:32 AM)MMKS Wrote: [\[CITE\]](#) I'm truly sorry for my mistakes... Im in a rush to take down the scammers, can you elaborate how can I use this tool sir ?

Did you read the article?