

Forum:[Hack Forums](#)

Thread: [UAC Bypass on Windows 11 - ctfmon -> MsCtfMonitor -> ACTX / tcmsetup -> tapi32](#)

Hackers - February 6, 2025, 10:19 pm

CVE-2024-6769

~ Got bored of politics for a sec. Here's a UAC instead ~

Confirmed Working - As of 2/15/2025

Quote:A DLL Hijacking caused by drive remapping combined with a poisoning of the activation cache in Microsoft Windows 10, Windows 11, Windows Server 2016, Windows Server 2019, and Windows Server 2022 allows a malicious authenticated attacker to elevate from a medium integrity process to a high integrity process without the intervention of a UAC prompt.

This requires the medium integrity-level privileges of an average user, and the account from which the attack is triggered must belong to the system's administrative group (the type of account that could level up to admin privileges, if not for UAC being in its way).

This CVE is still in the wild, and being researched - BUT is known by MS and ignored.

This method chains a few pieces together but pulls it off quickly.

~ Quickly for us, not so much for the original researchers ~

There are a couple things we have to do for the setup, but here's the CVE details:

<https://nvd.nist.gov/vuln/detail/cve-2024-6769>

Why is this CVE still able to be used?

It's simple. MS does not care.

Proof that MS does not consider UAC bypasses on admin accounts as 'hacking'. It's expected behavior:

Spoiler ([Click to View](#))

Quote:For its part, Microsoft acknowledged the research but said it does not consider this an actual vulnerability, because it falls under its concept of acceptability to have "non-robust" security boundaries.

"They see the admin-to-system boundary as a nonexistent boundary, because admin is trusted on a host." In other words, Microsoft doesn't consider CVE-2024-6769 a vulnerability if an admin user could ultimately perform the same system-level actions anyway, subject to UAC approval.

A Microsoft spokesperson highlighted that "The method requires membership in the Administrator group, so the so-called technique is just leveraging an intended permission or privilege which does not cross a security boundary."

"When UAC was introduced, I think we were all sold on the idea that UAC was this great new security feature, and Microsoft has a history of fixing bypasses for security features," he says. "So if they're saying that this is a trust boundary that is acceptable to traverse, really what they're saying to

me is that UAC is not a security feature. It's some sort of helpful mechanism, but it's not actually security related. I think it's a really strong philosophical difference."

This exploit (and most of the others like it) includes skipping the 'run as admin' prompt screen. However, MS has stated multiple times that they do not consider a 'skip' a severe exploit because they say this feature is for quality of life - security related, but not technically for total security. In other words, they know people will bypass the UAC prompts. Their recommendation is to lock down your account or use a non-admin account if you are concerned.

Different problem, same answer on CVE-2007-3463

Quote:the vendor states that "RunAs and UAC are convenience features, not security boundaries. If you need a security guarantee, please log out and log back in with a different account."

In other words, a UAC bypass is not considered an actual vulnerability.

Technically this is a whitehat guide.

1. ctfmon.exe has a DLL search priority bug. (CWE-426 : <https://cwe.mitre.org/data/definitions/426.html>)
2. It uses a bad match on a loaded DLL. We'll come back to this.
3. In your project folder, create an empty fake directory ".\windows\system32". There's also a low level symlink method around for writable system dir.
4. The method uses a fake MsCtfMonitor.dll with 1 function: DoMsCtfMonitor
5. Use ShellExecute to execute ctfmon.exe
6. Hook to intercept the process creation from ctfmon.exe
7. Remap C: inside of this hook, so that the system directory is changed when the process is suspended.
8. Resume the process creation
9. The custom DLL runs, payload is fired!
10. I'll stop numbering now, the next part is best described by the experts. Check the links I've included.

At this point of the method, we're close but not quite there. You will have high integrity for your runtime, but not full admin perms yet. This is where the cache poisoning method comes in to finish the method off.

I highly recommend you read all of the guides and CVE details before doing anything. However, what you are essentially looking for is to chain the ctfmon method into the ACTX cache method.

When ctfmon starts a ACTX request, it runs with RID 0x3000.

To do this, we will need the same or higher RID than the process that will use it. From what I'm reading this is due to a MS change in 2022, but as long as we solve the RID # then the method works (they solved it, don't worry).

Now, someone else did all this hard work for us obviously, so don't thank me.

tcmsetup also has 0x3000 RID, so we can use that.

And tcmsetup will then load in tapi32.dll.

The method uses a manifest XML file to trick tapi32 into loading imm32.dll. The method also requires a few other aspects of the files to sync up, including the resource name, language, last write time, and more.

Read this guide for all the RE data for more info on this part of the method

<https://www.coresecurity.com/core-labs/articles/cve-2024-6769-poisoning-activation-cache-elevate-medium-high-integrity>

Video demo: <https://github.com/fortra/CVE-2024-6769/blob/main/CVE-2024-6769.mp4>

POC:

<https://github.com/fortra/CVE-2024-6769>

--> <https://github.com/fortra/CVE-2024-6769/tree/main/SOURCES>

NOTE: I did spend some hours working on the POC. Each method works on its own, but I had to make sure to add a missing header file and make some code fixes for my Visual Studio to compile properly.

I may release my version in the future, but this method is still so fresh. I think anyone who is capable of programming can figure it out, but this is definitely NOT a UAC for beginners. You'll also need to think about using lay of the land methods, memory or thread/process methods, or other similar advanced topics alongside this method.

Further Research:

Spoiler ([Click to View](#))

https://static.bluefrostsecurity.de/files/lab/I_am_high-presentation.pdf

<https://labs.bluefrostsecurity.de/windows-system-drive-remapping-elevation-of-privileges>

<https://github.com/bluefrostsecurity/Windows-Drive-Remapping-EoP>

<https://www.coresecurity.com/core-labs/articles/cve-2024-6769-poisoning-activation-cache-elevate-medium-high-integrity>

<https://www.darkreading.com/vulnerabilities-threats/exploit-chain-windows-uac-bypass>

<https://www.zerodayinitiative.com/blog/2023/1/23/activation-context-cache-poisoning-exploiting-csrss-for-privilege-escalation>

<https://www.fortra.com/security/advisories/research/fr-2024-002>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-6769>

Related:

<https://securelist.com/windows-vulnerabilities/112232/>

<https://project-zero.issues.chromium.org/issues/42451595>

Hackers - October 18, 2025, 8:28 am

I spent a lot of time on this back then, and it worked well. Surprised this didn't get more attention, but it's really complicated to execute so that might be why

BlueBerryElite - October 23, 2025, 2:30 am

This looks high-quality, thanks for sharing it.

Hackers - October 28, 2025, 6:38 pm

(Oct 23, 2025 02:30 AM)BlueBerryElite Wrote: [\[CITE\]](#) This looks high-quality, thanks for sharing it. No problem! It's complicated, but it did work for me in several months ago & Windows/MS had no intent to patch it.

SpiderSpicy - January 19, 2026, 5:16 pm

(Oct 28, 2025 06:38 PM)nodes Wrote: [\[CITE\]](#) No problem! It's complicated, but it did work for me in several months ago & Windows/MS had no intent to patch it.

You are a real Genius my dude. Thanks lot for your amaizing job here. ?

Hackers - January 21, 2026, 12:20 pm

(Jan 19, 2026 06:16 PM)SpiderSpicy Wrote: [\[CITE\]](#) You are a real Genius my dude. Thanks lot for your amaizing job here. ?
thanks, I appreciate it!

Stanley - March 16, 2026, 8:39 am

I'm Stanley HF's helper bot. The OP (original poster) of this thread wants everyone to see this page and has elected to bump it to the top of the showthread listing. Since HF doesn't want a ton of LQP (Low Quality Posts) this is the best method of bumping your content. There is a small ?yte fee for each bump. Any OP can bump any of their threads on HF from the linked icon on the top of their first post.

If you haven't already read the first post of this thread we encourage you to do so.

Thanks,
Stanley