

Forum:[Hack Forums](#)

Thread: [Notepad++ DLL Hijack \(CVE-2025-56383\) Local Code Exec via Malicious Plugin DLL](#)

JoseMar - September 29, 2025, 2:38 am

Notepad++ DLL Hijack (CVE-2025-56383)
Local Code Exec via Malicious Plugin DLL

Okay, shorter: someone found CVE-2025-56383, it's a DLL-hijack-ish problem with Notepad++. PoC exists (yes, people posted it). It's not a worm that travels by itself. It is a really clean persistence trick if an attacker already has write access to where Notepad++ expects a DLL. So: not immediate doom for everyone, but it's the sort of thing you wake up to on a Monday and go, "oh great, another thing to babysit."

What the hell is a DLL hijack, again? (short version)

You know the drill, but let's not assume. Windows apps load DLLs. If the app doesn't say "load C:\Program Files\Notepad++\plugins\NppExport\NppExport.dll" and instead relies on the system search path or relative loading, Windows might look in places you didn't expect. Put a malicious DLL with the same name in an earlier-searched place --> app loads the wrong DLL --> attacker code runs under your user.

It's boringly elegant. Nothing flashy. No 0-day teleportation. But: every time you click Notepad++, that payload gets a ride. Persistence without noisy registry hacks, less likely to trip dumb AV. Sneaky.

Is this a catastrophe? (context matters, always)

Depends. If you're a freelancer using Notepad++ to patch a config file and you run as a local admin like it's 2005, sure, higher risk. If you're a corp with locked-down Program Files, app whitelisting, EDR, SIEM alarms, this is more like "useful footnote for IR." Neither answer is wrong.

Think of it like a spare key under the mat. If somebody already slipped into your house through a loose window (phish, RAT, whatever), planting that DLL is the spare key: opens the same door later, quietly. But if your house has proper locks, and the mat has been thrown out, the spare key doesn't help an outsider who can't get inside in the first place.

Also: Notepad++ is everywhere. That's the kicker. Attack surface scales with popularity. So the impact is multiplicative in the availability of the app, not necessarily the severity of the bug itself.

What can people actually do without losing their minds?

Practical, not paranoid: Update when the vendor patches. I know, I know, "update" is the most boring advice. But it's still the right one.

Lock down write access to program/plugin directories. If someone local can write there, you have bigger problems already, but this one reduces noise.

Use file integrity monitoring (FIM) if you're in an org. Not sexy, but it tells you when that NppExport.dll suddenly changes size from 600KB to 12KB overnight.

Consider app whitelisting (even basic SmartScreen / Defender Application Control stuff). Yes it's a deployment pain. Yes it stops dumb things.

For personal machines: don't run random installers. Use Chocolatey or winget if you want a slightly less sketchy install path. And maybe stop running as admin unless you're compiling a kernel or doing something actually privileged.

Small, realistic wins. Not an immediate silver bullet, but they limit attackers' options.

Ethics / disclosure thoughts

Researchers releasing PoCs are walking a line. On one hand, PoCs push vendors to patch faster, "look, this is real." On the other, they feed low-effort attackers. I'm not going to moralize too hard because I know people on both sides of this fence: finding things, tipping vendors, waiting for fixes, getting impatient, the whole loop.

That said: responsible disclosure is still better than screaming on Twitter and dropping a full repo with DLL source and build instructions. We can pressure devs without writing the instruction manual for the next script kiddie.

My two cents, messy and unfinished (like life)

I like small tools. I like them because they're fast and do one thing well. But we glorify lightweight apps and forget that Windows' "helpfulness" (search-first loader behavior, permissive write ACLs back in the day) is also what made them convenient. Fixing this is a teamwork problem: devs tighten load paths, packagers respect secure install locations, admins do the boring config work, users stop installing random crap.

Will that happen overnight? No. Probably some will patch, some won't, some admins will be like "eh." And then someone will use this as a stepping-stone in an attack chain and we'll have a fun postmortem to read over coffee.

Anyway, I'm done rambling for now. If you've poked around this and have non-exploit details (e.g., detection heuristics, weird timestamps, unusual DLL sizes) post them. If you're just here to shout "UNINSTALL NOTEPAD++", cool take, but also not helpful.

CVE-2025-56383-Proof-of-Concept (Not tested)

<https://github.com/zer0t0/CVE-2025-56383-Proof-of-Concept>

Money- - September 29, 2025, 4:20 am

I guess is pretty much your usual DLL Hijacking type of POC. Privilege escalate via the DLL if its the notepad++ is executed via admin etc...

ttbr0 - September 30, 2025, 4:43 am

this is stupid just like all the dll hijacking cves. mitre continue to act like clowns. it is legitimately a feature, not a bug. working as intended.

JoseMar - September 30, 2025, 5:59 am

(Sep 29, 2025 04:20 AM)Money- Wrote: [\[CITE\]](#) I guess is pretty much your usual DLL Hijacking type of POC. Privilege escalate via the DLL if its the notepad++ is executed via admin etc...

(Sep 30, 2025 04:43 AM)ttbr0 Wrote: [\[CITE\]](#) this is stupid just like all the dll hijacking cves. mitre continue to act like clowns. it is legitimately a feature, not a bug. working as intended.

Yes, this is already listed on GitHub with its CVE I haven't checked this. It's a pretty typical example, nothing special. Just a proof of concept. Still, it's a good reminder of how common DLL hijacking can be.

It's just a demonstration, not an exploit?

ttbr0 - October 1, 2025, 12:44 am

(Sep 30, 2025 05:59 AM)JoseMar Wrote: [\[CITE\]](#) Yes, this is already listed on GitHub with its CVE I haven't checked this. It's a pretty typical example, nothing special. Just a proof of concept. Still, it's

a good reminder of how common DLL hijacking can be.

It's just a demonstration, not an exploit?

i had another look and its not even dll hijacking. it is replacing the file on disk. mitre needs to be lobotomized for committing these sins.

Tyr - October 18, 2025, 4:32 am

(Sep 30, 2025 04:43 AM)ttbr0 Wrote: [\[CITE\]](#) this is stupid just like all the dll hijacking cves. mitre continue to act like clowns. it is legitimately a feature, not a bug. working as intended.

It exploits a known behaviour of the OS, but the application/installer is at fault for not handling that securely. Technically they are valid CVE's although I see your point.

Hackers - October 18, 2025, 8:35 am

(Sep 30, 2025 04:43 AM)ttbr0 Wrote: [\[CITE\]](#) this is stupid just like all the dll hijacking cves. mitre continue to act like clowns. it is legitimately a feature, not a bug. working as intended.

(Oct 1, 2025 12:44 AM)ttbr0 Wrote: [\[CITE\]](#) i had another look and its not even dll hijacking. it is replacing the file on disk. mitre needs to be lobotomized for committing these sins.

(Oct 18, 2025 04:32 AM)Tyr Wrote: [\[CITE\]](#) It exploits a known behaviour of the OS, but the application/installer is at fault for not handling that securely. Technically they are valid CVE's although I see your point.

I think I understand what you guys are saying, but Notepad++ is a trusted program that may be used by devs for editing code, and perhaps with admin perms. Even without admin, I could kind of see how this is not the worst CVE in the world, but also could still be useful.

> probably too obscure / too many steps to really be super effective

> easily sig detected once known / it is known

How many programs do people install in random dirs? You might be surprised. But that's not the main point I want to make

It would be tough to take advantage of this if Notepad is in a protected folder that would just throw more flags / detections if a program attempts to edit... lol

There are a lot of CVEs where the actual opportunity is tiny because of the requirements. This might be one of them, but not sure...

I could see how maybe someone could load in a new version of Notepad++ to be installed in a writable dir so that the DLL method can be used alongside an otherwise certified/signed program?

Here's a POC that shows the method being used on a new install of Notepad++, in a regular or new dir:

<https://github.com//zer0t0//CVE-2025-56383-Proof-of-Concept>

You're not required to limit yourself to only a pre-installed program. This could throw other flags obviously if sig detected, but just figured I'd mention it.

Here's a discussion about using Powershell to silently install Notepad:

<https://stackoverflow.com/questions/50274909/unattended-silent-install-notepad>

I think someone could create a chain method probably to make use of something like this.

I could be wrong, and not going to go too deep into this one because i'm focusing on Mac right now...

But I agree overall with ttbr0 and Tyr, this is not the deadliest method.
Still worth looking into though imo because of how popular NPP is

Lowkey - October 18, 2025, 8:38 am

I think I just got infected learning about this via this thread.

Hackers - October 18, 2025, 8:40 am

(Sep 30, 2025 04:43 AM)ttbr0 Wrote: [\[CITE\]](#) this is stupid just like all the dll hijacking cves. mitre continue to act like clowns. it is legitimately a feature, not a bug. working as intended.

(Oct 18, 2025 08:38 AM)Lowkey Wrote: [\[CITE\]](#) I think I just got infected learning about this via this thread.

Imao, it is a very official thread for a small method, but better than this for the 10,000th time:

If this thread leads to someone learning, then that's good.

I don't think methods always need to be the worst hack in the world to be useful.

Someone out there can still learn about DLL loading methods with this thread as a reference. I'm sure there are plenty of people who aren't even aware that programs still load dependencies like this.

I'm sure there are a number of users on this forum that don't even know what a DLL is, or what Notepad++ is compared to Notepad.exe.

Js lol

salmagamal2021 - October 19, 2025, 10:00 am

good topic thanks in advance

Tyr - October 19, 2025, 9:56 pm

(Oct 18, 2025 08:38 AM)Lowkey Wrote: [\[CITE\]](#) I think I just got infected learning about this via this thread.

I have a lot of diseases so I wish you the best.

(Oct 18, 2025 08:40 AM)enki Wrote: [\[CITE\]](#) Imao, it is a very official thread for a small method, but better than this for the 10,000th time:

If this thread leads to someone learning, then that's good.

I don't think methods always need to be the worst hack in the world to be useful.

Someone out there can still learn about DLL loading methods with this thread as a reference. I'm sure there are plenty of people who aren't even aware that programs still load dependencies like this.

I'm sure there are a number of users on this forum that don't even know what a DLL is, or what Notepad++ is compared to Notepad.exe.

Js lolDon't throw homeboy in the white under the bus that way D:

Also, I highly doubt anyone will "learn," from this unless it relates to them. But hey, who knows? Perhaps they may gain awareness of how this type of attack can happen by looking at the vectorization methodology. However, I must say, it happened to someone I knew who ran a private server and used Notepad++ for almost everything.

Lefty - October 20, 2025, 1:07 am

Oh wow. Looking forward to giving this a proper read tonight. Cheers mate!

Lowkey - October 20, 2025, 5:08 am

Tyr how do I join the group you are in now, asking for a friend.

Tyr - October 20, 2025, 12:41 pm

(Oct 20, 2025 05:08 AM)Lowkey Wrote: [\[CITE\]](#) Tyr how do I join the group you are in now, asking for a friend.

You gotta be canine mate. Is your friend a canine?

Lowkey - October 20, 2025, 3:16 pm

(Oct 20, 2025 12:41 PM)Tyr Wrote: [\[CITE\]](#) You gotta be canine mate. Is your friend a canine?
I know a few dogs.

Tyr - October 20, 2025, 7:50 pm

(Oct 20, 2025 03:16 PM)Lowkey Wrote: [\[CITE\]](#) I know a few dogs.
Shoot me a DM then sir. We shall evaluate whether these dogs are HQ or not.