

Forum:[Hack Forums](#)

Thread: [Zoom Bug Lets Attackers Jump to Admin in 1 Click, CVE-2025-49457](#)

JoseMar - August 12, 2025, 4:15 pm

Zoom Bug Lets Attackers Jump to Admin in 1 Click
CVE-2025-49457

So Zoom just dropped a fun little surprise in their security bulletin. Turns out there's a bug in the Windows client that lets an attacker basically waltz into higher privileges without needing to know your password or already be on your system.

It's got one of those official scary names, CVE-2025-49457, and a CVSS score of 9.6, which is basically "congratulations, your system is toast." The root problem? An untrusted search path. Translation: Zoom is sometimes willing to grab files from the wrong place, which means if you put something malicious where it thinks it should be looking, it'll run it.

Imagine ordering food from a restaurant, but instead of checking the bag, you just grab the first thing that smells like your order, even if it came from a random stranger on the street. That's this bug.

And it's apparently not that hard to trigger. Click the wrong meeting link, open the wrong file, and you're done. No 12-step phishing scam, no complicated exploit chain. Just... click.

Why This One Feels Worse Than Usual

It's not that this is some brand new, never-before-seen trick. DLL hijacks and path issues are ancient history in infosec terms. But it's Zoom. Everyone has Zoom. It's in offices, classrooms, courtrooms, therapy sessions. If you're targeting a big pool of people, this is a goldmine.

And because Zoom's client is running in so many different environments, an attacker doesn't need to be super picky. It's like fishing in an overstocked pond, just throw a line in and something will bite.

The kicker? Zoom's own offensive security team found this. Which is good, I guess, but it also means it could have been sitting there for years until someone got bored enough to dig.

The Problem With "Just Update"

Yeah yeah, the fix is "update to 6.3.10 or later." But in the real world, tons of people won't. Half the companies I've seen still have old Zoom builds because "we're waiting for IT approval", which is corporate speak for "we forgot about it and it's not on fire yet."

And regular users? They'll click "remind me later" until their machine dies of old age. We've all done it. Updates always feel optional until your system starts acting weird and you're suddenly Googling why your webcam is on by itself.

If I Were an Attacker...

This is basically a buffet of attack vectors. Stick a malicious file in a shared folder, or bundle it with "free HD Zoom backgrounds" and wait. You don't need to be clever, you just need to put it where

Zoom looks.

Pair this with a halfway decent phishing email and you could land inside a corporate network before lunch. Once you've got elevated privileges, you can do the fun stuff, install persistent malware, pivot deeper, grab credentials.

What's Actually Going to Happen

Some people will patch today. Some will patch in a few months. And some will never patch at all because they "barely use Zoom anyway." Those are the same people who think locking their front door is optional because "this neighborhood is safe."

By the time everyone's updated, someone will have found the next one. That's just the cycle. It's not a Zoom problem, it's a software problem.

So yeah, update if you care. Or don't. Just don't be shocked if someday your Zoom meeting freezes and your CPU usage spikes to 100%.

Jamika - *August 12, 2025, 4:19 pm*

I had zoom before on my work tablet, now i use Microsoft teams

0xEIPadrino - *August 13, 2025, 10:56 am*

your writeups always good to read thanks for sharing brother :)

HerrWinston - *August 13, 2025, 3:04 pm*

fascinating read, thanks and your right you dont wanna know how many websites are on "remind me" lol even on my laptop i have 3 updates queued lmao

K4RM4 - *August 15, 2025, 11:15 am*

As always, very interesting read. Thank you for sharing!

u00s - *September 12, 2025, 7:24 pm*

very interested, thank you