

Forum: [Hack Forums](#)

Thread: [WordPress Elementor CVE-2025-8489 Critical Admin Takeover Vulnerability](#)

JoseMar - December 3, 2025, 8:39 am

WordPress Elementor CVE-2025-8489
Critical Admin Takeover Vulnerability

Anyone Else Watching This King Addons Mess?

Honestly, I wasn't even planning to post today, but this whole King Addons for Elementor thing has me side-eying my installs harder than usual. Like, I know WordPress plugins are basically random loot boxes of "hope this doesn't nuke your site", but man, CVE-2025-8489 feels like someone pulled the You Lose Everything card.

I was reading through the notes and, yeah, unauthenticated admin creation. Of course. Because apparently the plugin just kinda shrugs and lets anyone toss "administrator" into a request like it's ordering a pizza. No login, no proof, just vibes. And with 10k+ installs? Great.

Just check this how stupidly simple the attack is. The hacker can send a crafted request to the WordPress admin-ajax.php endpoint and set the "user_role" field to "administrator" boom. I mean, who thought that was a good idea? Did someone just forget a permission check on a Friday and push it live anyway? I've done my share of sloppy deploys, but this is wild.?

Attack Traffic Going Nuts?

Wordfence is apparently blocking like 48k+ attempts already, which, okay, impressive numbers I guess, but also terrifying? Especially seeing specific IPs hammering the vuln like they're trying to speedrun a takeover. 45.61.157.120 pulling almost 30k on its own feels... obsessive.

Kinda makes me think about all the abandoned sites still running version 24.whatever because the owner got bored around 2022 and never logged in again. Those poor things don't stand a chance. The patch dropped late September 2025, but attackers waited until public disclosure in late October then immediately went feral. Well, still annoying.

If You're Running This Plugin, Seriously...

Update it. Like now, not "when I have time". And maybe check your admin list for random "Mario" or whatever. Anyway, I'm curious if anyone here actually saw live exploitation on their logs. I'm half expecting more waves later this month. Or maybe I'm being dramatic, I don't know. Just feels like one of those things that's gonna keep popping up in cleanup requests for a while.

Drop your stories if you've had to deal with this plugin chaos yet. Might as well compare notes before the next plugin decides to implode.

Hackers - December 3, 2025, 8:41 am

saw this come through in email alerts yesterday and had to notify a few old clients.

Seems like a huge vuln for such a popular plugin

JoseMar - December 3, 2025, 8:56 am

(Dec 3, 2025 09:41 AM)nodes Wrote: [\[CITE\]](#) saw this come through in email alerts yesterday and had to notify a few old clients.

Seems like a huge vuln for such a popular plugin

Yeah, Elementor is huge, and there are a ton of sites using it. A friend of mine has the plugin too, so I told him it's vulnerable. You know what he said?

"Nah, my site is just a simple website, nobody's gonna hack it..."

I was like, what?? ??? That makes zero sense. His clients literally visit that site to contact him directly. Sure, he's not running an online store, but all that traffic can be redirected somewhere else in seconds, or an attacker could just change the notification email and he'd never notice...

Some people just don't understand how the internet actually works. ?

Hackers - December 3, 2025, 9:11 am

(Dec 3, 2025 09:56 AM)JoseMar Wrote: [\[CITE\]](#) Yeah, Elementor is huge, and there are a ton of sites using it. A friend of mine has the plugin too, so I told him it's vulnerable. You know what he said?

"Nah, my site is just a simple website, nobody's gonna hack it..."

I was like, what?? ??? That makes zero sense. His clients literally visit that site to contact him directly. Sure, he's not running an online store, but all that traffic can be redirected somewhere else in seconds, or an attacker could just change the notification email and he'd never notice...

Some people just don't understand how the internet actually works. ?

yeah.... Sir, people scan for any site, even if that site only gets a small amount of traffic, that can be combined in a giant network of hacked sites.

He should reconsider his stance :)

Or at very least, implement a strict cache that prevents WordPress changes from going live w/o his approval.