

Forum:[Hack Forums](#)

Thread: [WordPress another day, another XSS \(LiteSpeed Cache CVE-2025-12450\)](#)

JoseMar - October 29, 2025, 2:56 pm

WordPress another day, another XSS
(LiteSpeed Cache CVE-2025-12450)

LiteSpeed Cache XSS, not surprised, but kinda disappointed

So apparently LiteSpeed Cache got hit with a reflected XSS (CVE-2025-12450). Big whoop, right? Another week, another plugin leaking user sessions like it's 2014 again.

But the thing is , this one actually matters. 7 million+ installs. That's not niche; that's grandma's cooking blog and the random local pizza shop all running the same plugin that now lets anyone inject JS if they click the wrong link.

And yeah, it's "just reflected," so you need user interaction, blah blah blah. But let's be real , users click everything. Someone could disguise it behind a tinyurl and half the admin population would fall for it before lunch.

What bugs me isn't even the vuln itself, it's how predictable it feels. Like, LiteSpeed is a massive player. You'd think by now every plugin touching output should by default sanitize and escape everything twice. It's 2025. We've been doing this dance since MySpace profiles had blinking text and autoplay music.

The "it's only medium severity" mindset
CVSS 6.1. Medium. That's the joke, right? Everyone reads "medium" and thinks "eh, we'll patch it next sprint." Except medium in this case means "millions of cached pages potentially serving malicious payloads."

I get that reflected XSS isn't as sexy as RCE, but combine it with social engineering and a lazy admin and you've got a neat little attack chain. Click the wrong URL, get session jacked, now someone's messing with your caching rules or dropping a crypto miner in your headers.

Maybe I'm overreacting, but the part that hits me is how long stuff like this flies under the radar. We depend on these plugins for speed, SEO, whatever... and one bad escape sequence later, your whole site's a toy.

The "just update" advice isn't enough
Sure, patch to 7.6, done deal. But you know what's wild? Half the sites running WordPress don't even know what version they're on. Their "developer" left in 2021, the admin password's in a spreadsheet somewhere, and auto-updates are off because "it broke the theme once."

That's the actual attack surface. Not the vuln itself, but the laziness, the inertia, the "we'll get to it later" attitude that keeps websec people busy.

Honestly, I don't even blame LiteSpeed. Everyone ships fast and breaks things now. But I do kinda wish plugin devs would stop pretending WordPress hardening is optional.

Anyway, that's my rant. Update your stuff, maybe audit your plugins once in a while, and if you're

feeling spicy, run your own WAF rules instead of trusting defaults.

Anyone here seen any live exploitation yet? Or are the kiddies still too busy poking at outdated Elementor builds?

leanas420 - November 3, 2025, 1:19 pm

which rat you crypted in the runtime scan you did.

goethe_71 - March 6, 2026, 7:44 am

Thanks for your sharing :) Anyway it's better to share examples for the clients?