

Forum:[Hack Forums](#)

Thread: [Chrome Fixes Another V8 Exploit \(Remote Code Execution Risk\) CVE-2025-9864](#)

JoseMar - September 3, 2025, 11:23 pm

Chrome Fixes Another V8 Exploit
(Remote Code Execution Risk) CVE-2025-9864

So Chrome just pushed out 140, and yeah, the headline is the “serious vulnerability patch.” Another RCE vector in V8, of course. Every time it’s the JS engine. Every time. I don’t even remember the last Chrome update where V8 wasn’t involved somehow.

The bug is tracked as CVE-2025-9864. Fancy way of saying “use-after-free,” which basically means Chrome kept a reference to something in memory after it had already been freed up. That’s like leaving your car running after you already gave the keys back to the valet. Eventually someone’s going to joyride it.

Anyway, Google patched it, rolled it out everywhere, and if you’re not updated yet, you’re technically walking around with a sign on your back that says “exploit me.”

But here’s the thing that bugs me:

The Constant Fire Drill

Does anyone else feel like these updates hit with the same rhythm as rain in Seattle? Like, every two weeks there’s some “critical flaw” in Chrome, it’s patched, and we all act surprised. But then two weeks later, rinse, repeat.

It makes me wonder... are we actually getting safer or just running in place? Sure, the bug is gone, but another one is sitting right behind it, waiting its turn. I get that software is complicated. I get that browsers are huge attack surfaces. But the whole cycle feels more like damage control than actual progress.

And here’s the funny part: you’ll see normal users in the wild (my parents, my roommate, whoever) not even bothering to update. They’ll keep 137 or 138 running until Chrome forces the update down their throat. Meanwhile, attackers know the patch notes exist, know the vulnerability class, and can reverse-engineer it. Who’s winning here? Not the users.

The Bug Bounty Thing

Google threw like 10k at the external researchers who found the bugs. That’s nice, I guess, but part of me laughs at how cheap that is compared to what some of these exploits could fetch on the black market.

Imagine: you’re some security researcher, you find a memory bug that can give someone full remote code execution, and you turn it in for a few grand and a shoutout in an advisory. Meanwhile, someone else could take that same bug and sell it to a broker for six figures easy.

Don’t get me wrong, responsible disclosure matters. But the economics are lopsided, and it’s a miracle anyone bothers playing nice.

The Takeaway (if there is one)

Yeah, update your browser. Do it now, because it's literally just a couple clicks away. But at the same time, don't fall into the trap of thinking that updating is some magic shield. It's not. It's plugging one hole while five more leaks are waiting.

I guess the bigger lesson is that Chrome, for all its shiny speed boosts and new features, is still fundamentally just this massive, messy pile of code that's always going to be a playground for researchers and attackers. Google knows it, we know it, and honestly, the hackers know it best.

Maybe that's fine. Maybe the constant treadmill is just the price of using a browser that tries to be everything at once. Or maybe one day people get tired of it and jump ship. Not that Firefox or Edge is some perfect alternative.

Anyway, that's my ramble. Just update your stuff. And maybe keep a second browser around for when the inevitable zero-day drops tomorrow.