

Forum:[Hack Forums](#)

Thread: [New Chrome Exploit Can Hijack Your System , Patch Now or Risk Everything](#)

JoseMar - July 23, 2025, 2:30 am

New Chrome Exploit Can Hijack Your System
Patch Now or Risk Everything

Chrome Users, Update Now

Google just dropped an urgent Chrome security update, and honestly, it's not something you want to ignore.

Even if you're the type who delays updates for weeks ("what's the worst that could happen?"), this one deserves a fast click on that "Update" button.

Why? Because three major security holes, two of them pretty scary, were just patched. And the kind of exploit these allow? It's the classic "visit a sketchy site, boom, game over" situation.

The Vulnerabilities (CVE-2025-8010 & 8011)

So here's the deal: both CVE-2025-8010 and CVE-2025-8011 are type confusion bugs inside Chrome's V8 JavaScript engine.

Discovered by Shaheen Fazim (yeah, legend), and reported July 9th.

To translate that from tech-jargon: the browser basically mixes up variable types in memory and that can, if you're unlucky, let someone run malicious code on your system. It's like handing over your keys because you thought the guy looked like a valet.

And Google knows it's serious: they dropped \$8,000 as a bounty for CVE-8010. (Second one's still being reviewed, but don't assume it's any less dangerous.)

What Is "Type Confusion" Anyway?

In human terms, it's like giving a screwdriver to someone who thinks it's a fork. Things break. Unexpected things happen. And sometimes, those "unexpected" things include remote code execution.

In V8, that means attackers can abuse how memory gets handled. And memory is sacred ground in browser security. You mess with it, you might get sandbox escapes, arbitrary code execution, heap corruption... all the nightmares.

Combine that with clever use-after-free chaining? Yeah, it's exploit party time.

Billions of Targets, One Engine

V8 isn't just Chrome. It's the engine inside Chromium-based browsers like Brave, Edge, and even

some gaming environments.

Every day, billions of scripts run through it.

It's no wonder attackers are targeting it. Google's bug bounties for V8 have hit \$20K for high-impact finds, and that alone should tell you what kind of playground this is.

The fact that someone found two high-severity bugs within a week? Alarming, but also... kind of expected in 2025.

The Bigger Picture: Vulnerabilities Are Rising

This isn't a Chrome problem. It's a 2025 internet problem.

Last year saw a 61% increase in browser-based security issues, and this year? We're already on track to hit 50,000 vulnerabilities globally across software.

Browser engines are growing more complex. Attack surfaces are ballooning. And let's be real, most people don't update unless the browser forces them.

That's a recipe for disaster.

What You Should Actually Do

This one's simple: Update Chrome. Right now.

Go to: Settings > About Chrome.

Let it auto-check, download, and restart.

You should be on version: 138.0.7204.168/.169 for Windows and Mac

138.0.7204.168 for Linux

Even if you're reading this from Brave, Edge, or any Chromium fork, same logic applies.

Because this kind of exploit doesn't need phishing emails or sketchy .exe files. Just one malicious webpage with weaponized JavaScript and... that's it.

Patching Is Self-Defense

This isn't fearmongering. It's just... reality.

Browsers are constantly at war with exploit devs, and you, the user, are in the crossfire whether you want to be or not.

So don't skip updates. Don't assume your adblocker saves you.

Let the devs fight the hard battles, your job is to click "Update" and reboot.

Sometimes, that's enough.

New entry for [7](#)contest?
? Big shoutout to [6](#) for making this even more exciting?

Hey guys, check this out.?

[DemonAsylum](#) [Immortal](#) [I N C R E D I B L E](#) [itcorp](#) [Jen](#) [vyactor](#) [Dystortion](#)

immeiron - July 23, 2025, 3:08 am

this was a very nice read

currently im using firefox and zen but im gonna update my .exe setup files for chromium browsers

Rax_ - July 23, 2025, 3:46 am

Thank you, haven't done an update in 2 days and you reminded me why I should stop being lazy and just make a cron for it.

Deezer - July 23, 2025, 5:03 am

Great write-up. Thanks for sharing.

JoseMar - July 23, 2025, 5:10 am

(Jul 23, 2025 03:08 AM)immeiron Wrote: [\[CITE\]](#) this was a very nice read

currently im using firefox and zen but im gonna update my .exe setup files for chromium browsers

(Jul 23, 2025 03:46 AM)Rax_ Wrote: [\[CITE\]](#) Thank you, haven't done an update in 2 days and you reminded me why I should stop being lazy and just make a cron for it.

(Jul 23, 2025 05:03 AM)Deezer Wrote: [\[CITE\]](#) Great write-up. Thanks for sharing.

Appreciate that?. I try to keep things honest and grounded, so it means a lot when someone takes the time to say thanks.

Also, don't forget to check my latest threads.?

Deezer - July 23, 2025, 5:39 am

I couldn't find info on which Chromium Engine Version has these CVEs patched. Would you happen to know?

Chornaya Magiya - July 24, 2025, 7:10 am

But far as i see they just lead to heap corruption and remote code execution in the renderer only.

That means they are still inside sandbox and can't execute OS level commands.

Real 2025 threat for chrome was CVE-2025-5419

ellectra - July 24, 2025, 10:00 am

Thanks for sharing