

## Forum:[Hack Forums](#)

Thread: [Chrome Hit with 2 High-Risk Vulns \[CVE-2025-5958 & CVE-2025-5959\]](#)

JoseMar - June 11, 2025, 5:51 pm

Chrome Hit with 2 High-Risk Vulns  
[CVE-2025-5958 & CVE-2025-5959]

So, yeah, another week, another critical Chrome update.

Google just pushed a security fix to patch two high-severity bugs in the desktop version of Chrome (for Windows, Mac, and Linux). The patched version is 137.0.7151.103 (or .104 for some platforms). It's rolling out now, but honestly, if you're reading this and haven't updated yet... You probably should.

I know. Boring. But hear me out.

The first one: CVE-2025-5958  
Use-After-Free in Media Component

This one's nasty. Basically, Chrome's media component messes up memory handling; it frees up an object, then still tries to use it later. Classic use-after-free stuff.

A researcher from Ant Group found it and got an \$8k bounty for it, which should tell you how seriously Google took this one. Imagine someone sending you a specially crafted media file embedded in a webpage. Chrome stumbles, mismanages memory, and boom, the attacker executes code on your system.

And that could mean anything from malware dropping quietly in the background to session hijacking, data theft, or whatever else they want to try.

Second one: CVE-2025-5959  
Type Confusion in the V8 Engine

Now, this one was reported during the Typhoon PWN live hacking event, which, if you're not familiar, is one of those "let's see what breaks" hacker cons. This vuln lets Chrome confuse one object for another, which sounds small, but it's not.

Because if the browser thinks something is a string when it's a memory pointer... bad things happen. Heap corruption, sandbox escape, remote code execution, pick your poison.

And again, all it takes is a malicious site. You click a link or land on the wrong ad, and it could be game over.

The bigger picture

These aren't theoretical bugs. They're the kind of issues you chain together in real-world browser exploits. If you're into malware dev, you'll probably recognize how powerful these primitives are.

Even if you're just browsing memes, vulnerabilities like this open doors for drive-by attacks,

meaning you don't have to download anything. Just visiting a site could be enough to get popped.

That's why Google isn't sharing full technical details right now. They usually wait until most people are patched. (Or until they're sure third-party code using the same libraries isn't affected.)

So... update your browser

Right now, manually checking for updates might be the fastest move:

Chrome menu > Help > About Google Chrome

It should start updating automatically from there.

This affects Chromium-based browsers too, like Edge, Brave, Vivaldi, Opera, so don't skip just because you're not using vanilla Chrome.

Google has already patched other critical bugs this year (like CVE-2025-5419 and CVE-2025-2783), and I don't think this will be the last. The pace of these vulnerabilities getting found, and sometimes exploited, is only getting faster.

Credit where it's due

Props to the security researchers for catching these before someone burned them in the wild. The \$8k bounty isn't life-changing, but it does keep the ecosystem somewhat honest.

If you're running anything that even smells like a browser exploit chain, I'd say keep an eye on this batch. Could see some interesting payloads emerge over the next month or two.

And if you're just trying to stay safe online? Well... don't wait on the auto-updater. Just update now.

Additional sources to explore:

You can also search directly on Google for more information:

<https://nvd.nist.gov/vuln/detail/CVE-2025-5958>

<https://cybersecuritynews.com/multiple-chrome-rce-vulnerabilities/>

<https://www.tenable.com/plugins/nessus/238069>

**Punisher** - June 11, 2025, 6:02 pm

Drive-by attacks in 2025, wow, not something you'd think you'd see these days.

Great share!

**Voidlight** - June 11, 2025, 6:29 pm

Nice share, I feel like with openai's o3 and onward we will be seeing a lot more of these popping up in the wild being used, not just some research lab finding it.

**Tyr** - June 11, 2025, 7:06 pm

(Jun 11, 2025 05:51 PM)JoseMar Wrote: [\[CITE\]](#) Ant Group found it and got an \$8k bounty for it  
For those who say threat bug bounty hunting doesn't payout in the end. This is also on the low end for this type of vuln too.

Anyway, great share TY.

**ttbr0** - June 11, 2025, 11:24 pm

pretty typical vulns you see for chrome. they are not problematic by themselves unless the attackers have inserted themselves into a website they want to steal data from it like in the form of an ad or injection like quantum attacks. if its a v8 vuln, you need to chain another vuln on top of it to do something useful. \$8k for the uaf suggests that it might not be that severe at all. its a pretty low payout compared to other vulns like in v8. for any attacks through the browser to get useful code execution on the machine, you need to chain at least 2 more vulns on top of either of these. realistically, this means nothing for the average user. the threat model is not even closely aligned with an attacker with these capabilities.