

Forum:[Hack Forums](#)

Thread: [The Chrome CVE-2025-6554 vulnerability](#)

Doc - September 20, 2025, 11:36 pm

So I recently came across a vulnerability (CVE-2025-6554) with unpatched Chrome versions (<138.0.7204.96) and started looking into it, and it's just crazy to me how a simple type confusion from a few lines of code opened the door to enable threat actors to create sites where this exploit would be the trigger for an entire chain that could give attackers access to your machine.

All that would be required on your part is navigating to the webpage.

To put it simply:

You wouldn't have to click on anything

You wouldn't have to interact with it in any way, shape or form

You would only have to visit the page and have it load

Since this is still being actively exploited in the wild and there are users still running unpatched versions of Chrome which are vulnerable to this (to give context, the patch for this exploit was released on June 30, 2025 for Windows and Linux; 138.0.7204.92 was released for macOS) I'm being intentionally vague about the details on why this is such a critical vulnerability.

There are very simple PoCs of this CVE on GitHub for those that want to take a look, but they are very limited in information about the vulnerability, for good reason.

I have plans to test on a VM to see a simplistic, non-actionable way of how this CVE would be exploited, but putting together anything showing how a potential exploit chain would be used is not something I'm going to do.

To give some context, there have already been at least 5 major Zero-Day vulnerabilities found in Chrome this year, and I respectfully decline to help individuals learn how to do any of this.

If you are still running a version of Chrome (whether it's on Brave, MS Edge, or the other browsers using Chrome) that is behind 138.0.7204.96, I highly recommend updating your browser as soon as you are able to. You can check by typing [chrome://version](#) in your browser's URL and hitting the Enter key.

If you are using Brave or another browser, the syntax may be different (for Brave it is [brave://version](#)) but I highly recommend checking the version your browser is using if it is using the Chrome engine.

After doing a deep dive on this and learning as much as I have, I thought I'd post it in here for anyone operating under the impression that you would have to actually click on a webpage, download, and then execute something to infect your machine. While what I stated above is commonly the case, there are cases like this one where you could potentially become infected by merely visiting a webpage using a vulnerable version of Chrome.

Anyway, I tried not to bother too much with the formatting of this post, but hope some find it a good read and update their browsers if they find they are vulnerable.

Feel free to let me know what you think, and remember to try your best to keep your shit up to date.

Hackers - *September 25, 2025, 12:32 pm*

Good call on V8 and general Chromium warnings

I forget how many browsers use it & are probably delayed on updates

Chorozon - *September 29, 2025, 6:59 am*

Good post OP thanks for the read

DAL-SHA - *September 29, 2025, 8:44 am*

such an interesting insight ! ??

me , myself im a bit away from the latest exploits but always open to read such topics ..