



**NATIONAL  
CSIRT CY**



**Google Chrome: Access of Resource**

**01/07/2025**

**Using Incompatible Type ('Type Confusion')**

## **CONFIDENTIAL**

The content of this document is intended solely for use by the natural or legal person to whom it is addressed. If you gain access to this document by mistake, you should be aware that any forwarding, copying or disclosure of its content to any other person is strictly prohibited, and you must inform the sender immediately.

## Executive Summary

Type confusion in V8 in Google Chrome prior to 138.0.7204.96 allowed a remote attacker to perform arbitrary read/write via a crafted HTML page.

## Analysis

When the product accesses the resource using an incompatible type, this could trigger logical errors because the resource does not have expected properties. In languages without memory safety, such as C and C++, type confusion can lead to out-of-bounds memory access.

## Common Weakness Enumeration

<https://cwe.mitre.org/data/definitions/843.html>

## Common Vulnerabilities & Exposures

<https://nvd.nist.gov/vuln/detail/CVE-2025-6554>

## Solutions

The Stable channel has been updated to 138.0.7204.96/.97 for Windows, 138.0.7204.92/.93 for Mac and 138.0.7204.96 for Linux which will roll out over the coming days/weeks.

Please distribute this information among your subsidiaries and partners, and also share with us any pertinent information and findings you may have (e.g IOCs, TTPs etc)

The Digital Security Authority extends its appreciation for the continued collaboration.

## Disclaimer

Organizations are advised to consult with relevant cybersecurity professionals and follow best practices for their specific environments.