Google Chrome Zero-Day Actively Exploited

TL;DR

Attackers are exploiting a new Chrome V8 type-confusion flaw that leads to heap corruption when someone is tricked into opening a malicious HTML page.

Google pushed an emergency update, and all users and organizations should update Chrome immediately and restart their browsers.

Overview

Google released a patch for a new Chrome zero-day, CVE-2025-13223 (CVSS 8.8), after its Threat Analysis Group confirmed active exploitation. The flaw is in Chrome's V8 JavaScript/WebAssembly engine and allows remote attackers to corrupt memory using crafted HTML or JavaScript delivered through malicious sites.

Impacted Products

- Google Chrome (Windows, macOS, Linux)
- Microsoft Edge (Chromium-based)
- Brave Browser
- Opera Browser
- Vivaldi Browser
- Any other Chromium-based browser using the V8 engine

CVE-2025-13223 is a type confusion issue inside V8. When V8 misidentifies an object's type, memory can be accessed incorrectly, allowing heap corruption triggered by malicious HTML or JavaScript. Attackers must convince targets to visit a crafted page, typically through phishing, drive-by redirects, or malvertising.

A second V8 issue, CVE-2025-13224, was also patched but has no confirmed exploitation to date. When attackers focus on browser exploits, it usually means they're trying to catch users during everyday browsing. With this kind of exploit, there are no login prompts, no file downloads, just one wrong click. Aspire recommends making sure your browser is updated as soon as possible.

Aspire Protects

- **Patch** – Update Chrome to version 142.0.7444.x immediately, then restart the browser to finalize the patch.

- Warn staff to avoid clicking unknown links, unexpected “document review” prompts, or redirect-heavy websites until updates are fully deployed.
- Apply upcoming updates to Edge, Brave, Opera, and other Chromium-based browsers as soon as they release patched builds. Vivaldi already has delivered a fix.

TTPs to Watch

Initial Access

- Drive-By Compromise [T1189] – The attacker may lure users to a malicious webpage containing crafted JavaScript or HTML designed to trigger the V8 type confusion vulnerability.

Execution

- User Execution: Malicious Link [T1204.001] – The attacker may rely on phishing emails or social engineering to convince the user to click a link that loads the malicious page.

Privilege Escalation

- Exploitation for Privilege Escalation [T1068] – If paired with a sandbox escape, the attacker may attempt to gain deeper access on the system.

Defense Evasion

- Exploitation of Vulnerability [T1210] – The attacker leverages the unpatched browser engine to run unauthorized actions inside the browser environment.

IoCs

There are no known IoCs at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how we can help protect your organization, contact Aspire’s Customer Success Management team.

Targeted Industries

Because Chrome is used across nearly every business environment, exploitation can affect any organization that relies on modern web browsers for day-to-day operations:

- Finance
- Government
- Education
- Energy
- Healthcare

- Retail
- Technology
- Manufacturing

Aspire's Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

Chrome Releases: Stable Channel Update for Desktop

CVE Record: CVE-2025-13223