Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

CVE-2026-85046: Chrome V8 Type Confusion Zero-Day Exploited in the Wild

Date of Publication	Admiralty Code	TA Number
September 04, 2026	A1	TA2026258

Summary

First Seen: August 2026
Affected Products: Google Chrome (Windows, macOS, Linux) prior to 152.0.7977.82/.83; Chromium-based browsers (Microsoft Edge, Brave, Opera, Vivaldi)
Impact: Google has patched CVE-2026-85046, a High-severity type confusion vulnerability in Chrome's V8 JavaScript and WebAssembly engine that is being actively exploited in the wild, with the fix shipped in Stable 152.0.7977.82/.83 for Windows and macOS and 152.0.7977.82 for Linux on September 3, 2026. Rated CVSS 8.8, the flaw allows a remote attacker to execute arbitrary code inside the sandbox via a crafted HTML page, with the researcher attributing the root cause to a compiler bug affecting both Maglev and TurboFan that yields an arbitrary read/write primitive on the JavaScript heap. Google has withheld attack details pending broad patch adoption, and no threat actor or targeting has been attributed. Organisations should update Chrome immediately and track fixes for other Chromium-based browsers, which share the vulnerable V8 code.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-85046	Google Chrome V8 Type Confusion Vulnerability	Google Chrome	✓	✗	✓

Vulnerability Details

#1 Google has confirmed that a V8 vulnerability in Chrome is under active exploitation and has shipped a fix in Stable 152.0.7977.82/.83 for Windows and macOS and 152.0.7977.82 for Linux, released September 3, 2026. Tracked as CVE-2026-85046 and rated High, the flaw is a type confusion bug in V8, the JavaScript and WebAssembly engine shared by Chrome and all Chromium-based browsers, and is one of 12 security issues resolved in this build.

#2 The CVE record assigns a CVSS score of 8.8 and describes the bug as allowing a remote attacker to execute arbitrary code inside the sandbox by luring a victim to a crafted HTML page. In a separate blog post, the researcher attributes the root cause to a compiler bug in which an array holding PACKED_ELEMENTS is assigned the PACKED_SMI_ELEMENTS map, yielding an arbitrary read/write primitive on the JavaScript heap, and notes the bug was present in both the Maglev and TurboFan compilers. This is researcher-reported and not yet confirmed by Google, whose bug tracker entry remains restricted. Such a primitive is typically chained with a separate sandbox escape to achieve full system compromise.

#3 Google has withheld attack details pending broad patch adoption, and no threat actor, malware or targeting has been attributed in the available reporting. This is reported to be the sixth actively exploited Chrome zero-day patched in 2026. Organisations should update Chrome immediately and track other Chromium-based browsers, which share the vulnerable V8 code and will ship fixes on their own schedules. Industry patch guidance likewise flags this release for priority deployment ahead of next week's scheduled Patch Tuesday cycle.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-85046	Google Chrome (Before 152.0.7977.82 Linux; Before 152.0.7977.82/.83 Windows, macOS)	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	CWE-843

Recommendations

Update Chrome Immediately: Upgrade all Chrome installations to 152.0.7977.82/.83 on Windows and macOS and 152.0.7977.82 on Linux. Users can force the update via More > Help > About Google Chrome and then Relaunch; enterprises should push the build through their management tooling rather than waiting for the staged rollout.

Patch Chromium-Based Browsers as Fixes Land: Microsoft Edge, Brave, Opera and Vivaldi share the vulnerable V8 code. Track each vendor's release channel and apply the corresponding update as soon as it is published; HKCERT has already issued a parallel Microsoft Edge bulletin on the same day.

Hunt for Exploitation Indicators: Because Google has confirmed in-the-wild exploitation but not published attack details, review browser process telemetry for anomalous renderer crashes, unexpected child processes spawned by chrome.exe or the equivalent, and outbound connections following visits to newly registered or low-reputation domains during the exposure window from at least August 4, 2026 onward.

Reduce Exposure Until Patched: Where immediate patching is not possible, restrict browsing to allow-listed destinations, enable Enhanced Safe Browsing, and consider temporarily blocking JavaScript on untrusted sites via Chrome's per-site content settings or the JavaScriptBlockedForUrls enterprise policy. These controls buy time during the rollout period, consistent with the network-as-control-plane approach highlighted in the September Patch Tuesday forecast.

Enforce Browser Update Policy: Configure Chrome enterprise policies to disallow update deferral and to relaunch within a defined window after an update is staged, so that future zero-days such as the six already patched this year are closed automatically.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1189: Drive-by Compromise	
Execution	T1203: Exploitation for Client Execution	
	T1059: Command and Scripting Interpreter	T1059.007: JavaScript
Resource Development	T1588: Obtain Capabilities	T1588.006: Vulnerabilities

Patch Link

https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_01882797386.html

References

https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_01882797386.html

https://www.hkcert.org/security-bulletin/google-chrome-multiple-vulnerabilities_20260904

https://serotav.github.io/Writeups/v8/when-sorting-leads-to-confusion/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of **HivePro**.

REPORT GENERATED ON

September 04, 2026 • 05:30 AM

© 2026 All Rights are Reserved by Hive Pro

More at www.hivepro.com