Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Google Rushes to Fix Actively Exploited Flaws

Date of Publication	Admiralty Code	TA Number
March 16, 2026	A1	TA2026072

Summary

First Seen: March 2026
Affected Products: Google Chrome
Impact: Google has issued urgent security updates for Google Chrome after confirming two high-severity vulnerabilities, CVE-2026-3909 and CVE-2026-3910. Notably, CVE-2026-3910 is currently being actively exploited in the wild. The flaws affect critical browser components, including the Skia graphics library and the V8 JavaScript engine, causing memory corruption or executing malicious code within Chrome's sandbox environment. While a fix for the V8 issue has already been released, the patch for the Skia vulnerability has been temporarily pulled from the latest update and will be delivered in a future release. Users are strongly advised to update their browsers immediately to reduce the risk of exploitation.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-3909	Google Skia Out-of-Bounds Write Vulnerability	Google Chrome	✓	✓	✗
CVE-2026-3910	Google Chromium V8 Improper Restriction of Operations Within the Bounds of a Memory Buffer Vulnerability	Google Chrome	✓	✓	✓

Vulnerability Details

#1

Google has issued urgent security updates to address two high-severity vulnerabilities affecting the Google Chrome browser, both of which have already been exploited in real-world attacks. The flaws, tracked as CVE-2026-3909 and CVE-2026-3910, highlight how widely used browser components remain targeted as entry points for sophisticated cyber operations.

#2

The first vulnerability, CVE-2026-3909, is an out-of-bounds write affecting Skia, the graphics library that renders most visual elements in Chrome, including images, text, and vector graphics. The flaw occurs due to insufficient bounds checking during memory write operations, allowing attackers to write data beyond the limits of allocated memory. A malicious actor can exploit this weakness by hosting a specially crafted HTML page that triggers the vulnerable rendering process. Simply visiting or being redirected to such a page could activate the exploit. The vulnerability impacts Chrome versions before 146.0.7680.75 on Windows, macOS, and Linux. Google has temporarily removed the fix from the 146.0.7680.75/76 release and plans to address it in a future update, meaning the issue remains unpatched for now.

#3

The second flaw, CVE-2026-3910, affects V8, the JavaScript and WebAssembly engine used by Chrome to execute web code. Classified as an inappropriate implementation vulnerability, the issue stems from a flaw in how V8 enforces certain security constraints. By exploiting this weakness through a specially crafted webpage, an attacker could achieve arbitrary code execution within Chrome's sandbox environment. While the sandbox restricts direct system access, such vulnerabilities are frequently used as the initial step in more complex exploit chains, where attackers combine them with additional flaws to escape the sandbox and compromise the underlying system.

#4

To mitigate potential risks, users should immediately update Chrome to version 146.0.7680.75/76 on Windows and macOS, or 146.0.7680.75 on Linux, where the fix for CVE-2026-3910 has already been applied. Updates can be installed by navigating to More → Help → About Google Chrome and relaunching the browser once the update is downloaded. Keeping browsers updated remains a critical defense, particularly as actively exploited vulnerabilities continue to surface in widely used web technologies.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-3909	Google Chrome (before 146.0.7680.75)	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	CWE-787
CVE-2026-3910	Google Chrome (before 146.0.7680.75)	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	CWE-94, CWE-119

Recommendations

Update Google Chrome Immediately: Install the latest stable release (146.0.7680.75/76 for Windows and macOS, 146.0.7680.75 for Linux) to remediate CVE-2026-3910. Users can navigate to More > Help > About Google Chrome to trigger the update and must relaunch the browser to apply the patch. This update does not address CVE-2026-3909, so continued vigilance and rapid patching of subsequent releases is essential.

Monitor for the CVE-2026-3909 Patch Release: Since Google has confirmed that the fix for CVE-2026-3909 has been deferred to a future Chrome update, organizations should closely monitor the Chrome Releases blog and their patch management systems for the forthcoming release. Once available, this patch should be prioritized for immediate deployment.

Update Chromium-Based Browsers: Organizations and users relying on Chromium-derived browsers such as Microsoft Edge, Brave, Opera, and Vivaldi should apply the corresponding security updates from those vendors as soon as they become available, as these browsers share the same vulnerable Skia and V8 components.

Restrict Browsing to Trusted Sites Where Feasible: For high-value or high-risk user segments, consider implementing browser isolation solutions or restricting access to untrusted web content to reduce exposure to drive-by exploitation scenarios that leverage these vulnerabilities.

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	
Resource Development	T1588: Obtain Capabilities	T1588.006: Vulnerabilities

Patch Link

https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_12.html

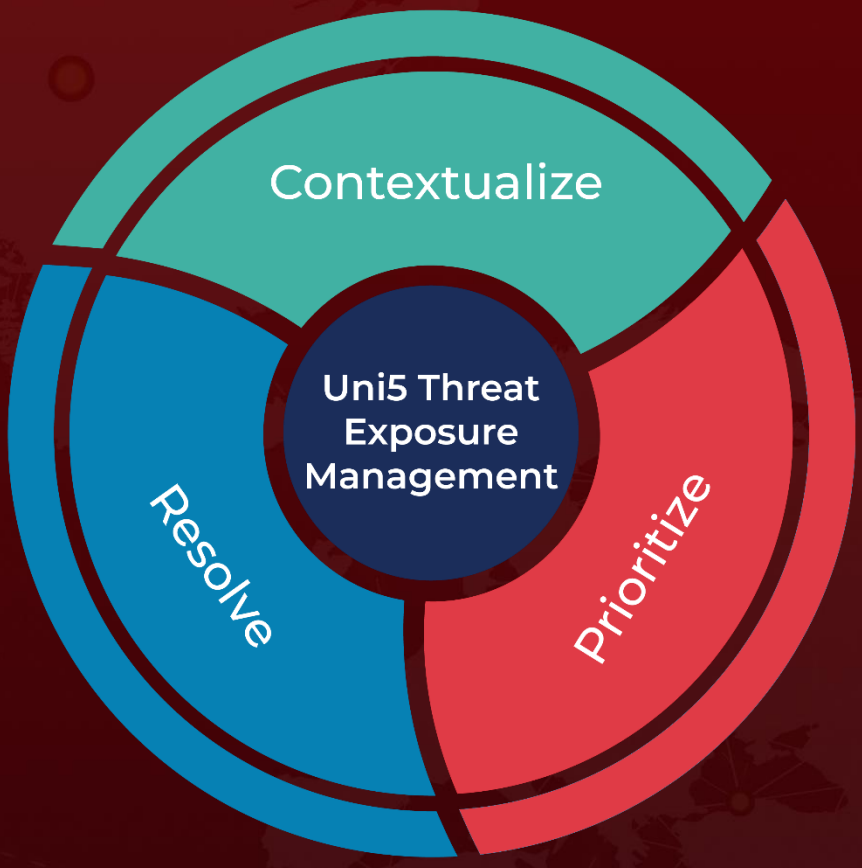
References

https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_12.html

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 free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

March 16, 2026 • 7:30 AM

© 2026 All Rights are Reserved by Hive Pro

More at www.hivepro.com