Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Google Chrome CSS Use-After-Free Zero-Day Vulnerability (CVE-2026-2441)

Date of Publication	Admiralty Code	TA Number
February 17, 2026	A1	TA2026045

Summary

First Seen: February 11, 2026
Affected Products: Google Chrome
Impact: A critical memory flaw tracked as CVE-2026-2441 is putting millions of browsers at risk, as attackers exploit a weakness in the CSS engine of the Chromium-based ecosystem to silently compromise systems through nothing more than a malicious webpage visit. By abusing a use-after-free condition, attackers can hijack browser behavior and execute harmful code with minimal user interaction, making routine web browsing a potential entry point for compromise. The issue originates in the rendering engine powering browsers built on Chromium, and Google has already confirmed that the vulnerability is being actively exploited, making immediate browser updates essential to stay protected.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-2441	Google Chromium CSS Use-After-Free Vulnerability	Google Chrome	✓	✓	✓

Vulnerability Details

#1

CVE-2026-2441 is a use-after-free (UAF) flaw, categorized under CWE-416, a class of memory safety issues that arise when software continues to use memory after it has already been released. This can lead to unpredictable behavior, allowing attackers to manipulate application memory, crash the program, or even run malicious code. In this case, the weakness lies in the Chromium rendering engine's CSS handling logic, with public analysis linking the issue to how CSS font feature values are processed in the browser.

#2

The vulnerability stems from faulty memory management within the browser's CSS processing logic, where an object is freed but still referenced through a lingering pointer. If that memory is later reused for another purpose, the stale reference can access or manipulate unintended data. Attackers can exploit this condition to influence application behavior and potentially redirect execution flow. This pattern is a well-known exploitation technique and has repeatedly surfaced in modern browser engines due to their complexity and performance-critical memory operations.

#3

In practice, exploitation typically occurs through a drive-by attack delivered via a specially crafted web page. Victims only need to visit a malicious or compromised website or be redirected via phishing or malicious advertising for the exploit to trigger. Once the page loads, the browser's CSS rendering pipeline processes the malicious content, activating the use-after-free condition and allowing attackers to execute code within the browser environment. No further action from the user is required beyond opening the page.

#4

All versions of Chrome affected before the patched releases are vulnerable across major platforms, and other browsers based on the same engine, including products from Microsoft, Brave Software, Opera, and Vivaldi Technologies, may also be impacted until vendors ship corresponding updates. The flaw originates in the open-source engine maintained by Chromium contributors, and Google has confirmed that the vulnerability is already being exploited in real-world attacks, underscoring the urgency of applying available patches.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-2441	Google Chrome (Before 145.0.7632.75 on Windows/macOS; Before 144.0.7559.75 on Linux)	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	CWE-416

Recommendations

Update Google Chrome Immediately: Apply the latest security patch by updating Chrome to version 145.0.7632.75 or later for Windows and macOS, and 144.0.7559.75 or later for Linux. For organizations using the Extended Stable channel, update to version 144.0.7559.177 or later. Users should navigate to More > Help > About Google Chrome to trigger the update, and critically, must restart the browser after the update to ensure the patched binary is active.

Prioritize High-Risk Endpoints for Patch Deployment: Identify and prioritize patching for endpoints that are most likely to be targeted, including systems used by executives, finance teams, IT administrators, SOC analysts, and other privileged users. These high-value targets are often the focus of sophisticated threat actors exploiting zero-day vulnerabilities, and their browsing patterns may increase exposure to drive-by attacks via spear-phishing links or watering hole campaigns.

Update Chromium-Based Browsers Across the Environment: Ensure that all Chromium-based browsers deployed in the environment, including Microsoft Edge, Brave, Opera, and Vivaldi, are monitored for vendor-specific security updates that incorporate the upstream Chromium fix. Do not assume these browsers are patched simultaneously with Chrome, as each vendor has its own release cycle and integration timeline. Track vendor advisories for each browser and apply updates as they become available.

Vulnerability Management and Continuous Assessment: Maintain an up-to-date inventory of all browser versions deployed across the organization and establish automated patch compliance reporting for critical browser updates. Evaluate the security posture of all software that embeds the Chromium engine, including Electron-based applications, to assess broader exposure to the underlying vulnerability. Implement a policy of regular vulnerability scanning and assessment to ensure timely identification and remediation of newly disclosed threats, particularly zero-day vulnerabilities with confirmed in-the-wild exploitation.

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/2026/02/stable-channel-update-for-desktop_13.html

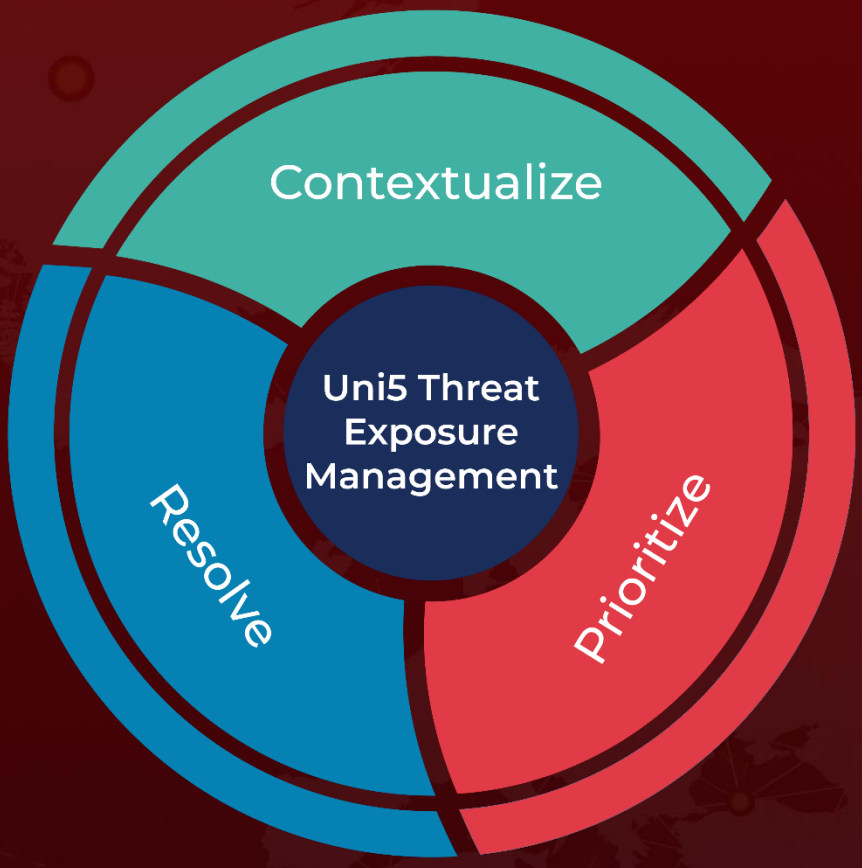
References

https://chromereleases.googleblog.com/2026/02/stable-channel-update-for-desktop_13.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

February 17, 2026 • 5:00 AM

More at www.hivepro.com