

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

CVE-2026-5281: Chrome Dawn Flaw Sparks In-the-Wild Zero-Day Attacks

Date of Publication

April 02, 2026

Admiralty Code

A1

TA Number

TA2026088

Summary

First Seen: March 10, 2026

Affected Products: Google Chrome

Impact: Google has rushed out emergency fixes for CVE-2026-5281, a Chrome zero-day already being exploited in the wild, rooted in a use-after-free flaw within the WebGPU-powered Dawn component. By mishandling memory during GPU operations, the bug leaves behind dangling pointers that attackers can abuse to execute arbitrary code. With active exploitation confirmed, updating Chrome immediately is critical to staying protected.

⚙️ CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-5281	Google Dawn Use-After-Free Vulnerability	Google Chrome	✅	✅	✅

Vulnerability Details

#1

Google released emergency updates to fix another Chrome zero-day vulnerability exploited in attacks, tracked as CVE-2026-5281. This flaw is a use-after-free (UAF) issue (CWE-416) in the Dawn component, which powers Chrome's implementation of the WebGPU API. Designed to enable high-performance GPU access from within the browser, WebGPU introduces complex memory interactions, making flaws like this particularly dangerous when memory is accessed after being freed.

#2

The vulnerability stems from improper memory lifecycle handling within Dawn during WebGPU operations. Certain GPU resources, once released, can still be referenced through lingering pointers. An attacker who has already gained a foothold in the Chrome renderer process can exploit this condition using a specially crafted web page with malicious WebGPU calls, ultimately triggering access to freed memory and achieving arbitrary code execution.

#3

The attack vector for this vulnerability is network-based, requiring user interaction; specifically, the victim must navigate to or be redirected to a malicious web page. However, because exploitation requires prior compromise of the renderer process, this vulnerability is most likely used as part of a multi-stage exploit chain, where an initial vulnerability is used to compromise the renderer sandbox before CVE-2026-5281 is leveraged for sandbox escape or privilege escalation to achieve full code execution on the host system.

#4

The issue affects Chrome versions before 146.0.7680.178 on Windows and macOS, and 146.0.7680.177 on Linux, as well as other Chromium-based browsers that include the vulnerable Dawn component. With active exploitation confirmed, users and organizations should immediately update to the latest Chrome version to reduce exposure and prevent potential attacks.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-5281	Google Chrome (Before 146.0.7680.178)	cpe:2.3:a:google:chrome:*.:*:*:*:*:*	CWE-416

Recommendations



Update Google Chrome Immediately: All users and organizations should update Google Chrome to version 146.0.7680.177/178 for Windows and macOS, or 146.0.7680.177 for Linux without delay. This patch resolves the use-after-free vulnerability in Dawn that is under active exploitation. To update, navigate to More > Help > About Google Chrome and allow the browser to download and install the latest version, then relaunch the browser to complete the update process.



Update Chromium-Based Browsers: Users of other Chromium-based browsers, including Microsoft Edge, Brave, Opera, and Vivaldi, should monitor their respective vendors for security updates addressing the same underlying vulnerability and apply patches as soon as they become available. These browsers share the Chromium engine and are equally susceptible to CVE-2026-5281 if running unpatched versions.



Enable Automatic Updates: Ensure that automatic update mechanisms are enabled for all browsers deployed across the organization. This minimizes the window of exposure between vulnerability disclosure and patch application and reduces reliance on manual intervention for critical security updates.



Vulnerability Management: Maintain a comprehensive vulnerability management program that includes regular scanning, patch prioritization based on CISA KEV listings and active exploitation status, and a defined SLA for critical patch deployment. Maintain an inventory of all browser versions deployed across the enterprise and establish processes for rapid response when zero-day vulnerabilities are disclosed.



Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	<u>T1189</u> : Drive-by Compromise	
Execution	<u>T1203</u> : Exploitation for Client Execution	
	<u>T1059</u> : Command and Scripting Interpreter	
Privilege Escalation	<u>T1068</u> : Exploitation for Privilege Escalation	
Resource Development	<u>T1588</u> : Obtain Capabilities	<u>T1588.006</u> : Vulnerabilities



Patch Link

https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_31.html



References

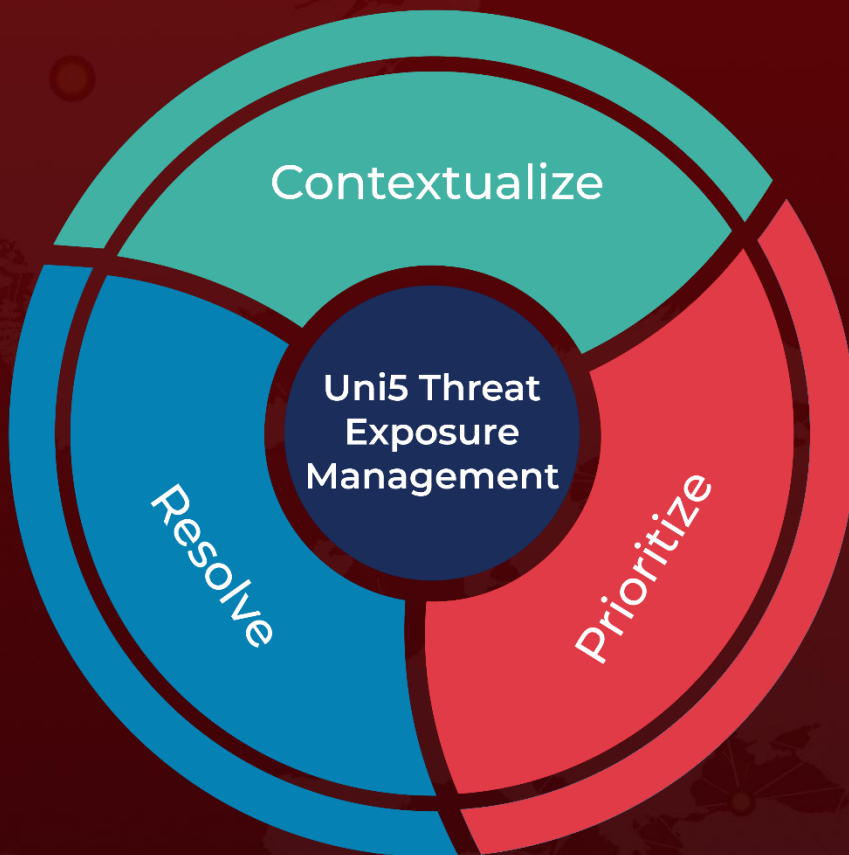
https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_31.html



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

April 02, 2026 • 08:30 AM

© 2026 All Rights are Reserved by Hive Pro



More at www.hivepro.com