Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Google Chrome Zero-Day Exploited in ANGLE Graphics Engine

Date of Publication	Last Updated Date	Admiralty Code	TA Number
December 12, 2025	December 15, 2025	A1	TA2025376

Summary

First Seen: December 10, 2025
Affected Product: Google Chrome
Affected Platform: Windows, macOS, Linux
Impact: Google released an emergency Chrome update on December 10, 2025 to fix three security vulnerabilities, including a high-severity zero-day in the ANGLE graphics engine that is already being exploited in the wild. The flaw allows buffer overflows that could enable memory corruption or code execution through malicious web content. Two additional medium-severity issues, in the Password Manager and Toolbar, were also patched. Because the zero-day affects all Chromium-based browsers and poses drive-by attack risks, users and organizations are urged to update immediately across Windows, macOS, and Linux.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-14174	Google Chromium Out of Bounds Memory Access Vulnerability	Google Chrome	✓	✓	✓
CVE-2025-14372	Google Chrome Password Manager Use After Free Vulnerability	Google Chrome	✗	✗	✓
CVE-2025-14373	Google Chrome Toolbar Inappropriate Implementation Vulnerability	Google Chrome	✗	✗	✓

Vulnerability Details

#1

Google released an emergency Chrome security update on December 10, 2025, for versions 143.0.7499.109/.110, addressing three vulnerabilities, including a high-severity zero-day (CVE-2025-14174) actively exploited in the wild. The critical flaw is a buffer overflow in Chrome's ANGLE graphics engine, specifically in the Metal renderer used on Apple platforms, stemming from improper buffer size calculations that can lead to memory corruption, crashes, or potentially arbitrary code execution. This marks Chrome's eighth zero-day patch of 2025, highlighting persistent targeting of browser graphics components.

#2

The zero-day poses significant risk because ANGLE processes untrusted graphics content from web pages, potentially enabling drive-by attacks via crafted input like WebGL, though exact exploitation chains remain undisclosed. Google has confirmed active in-the-wild exploitation but withheld full details under coordination with vendors, restricting access in the Chromium tracker. Given ANGLE's cross-platform use in Chromium-based browsers, organizations face elevated exposure until patches propagate across forks like Edge or Brave.

#3

Alongside the zero-day, Google patched two medium-severity issues: CVE-2025-14372, a use-after-free in Password Manager that may allow memory corruption under precise conditions, and CVE-2025-14373, an inappropriate implementation in Toolbar that could enable UI manipulation for phishing or spoofing. Both vulnerabilities were responsibly disclosed in November 2025 with and awarded bug bounties. These fixes underscore the need for immediate updates on Windows, macOS, and Linux to mitigate active threats across the ecosystem.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-14174	Google Chrome prior 143.0.7499.109 (Linux), BEFORE 143.0.7499.109/.110 (Windows/Mac)	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	CWE-122
CVE-2025-14372	Google Chrome prior 143.0.7499.109 (Linux), BEFORE 143.0.7499.109/.110 (Windows/Mac)	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	CWE-416
CVE-2025-14373	Google Chrome prior 143.0.7499.109 (Linux), BEFORE 143.0.7499.109/.110 (Windows/Mac)	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	CWE-358

Recommendations

Patch Deployment: Immediately update Chrome to versions 143.0.7499.109 (Linux) and 143.0.7499.109/.110 (Windows/macOS), pushing the update through enterprise tools. Confirm installation in “About Chrome” and ensure compliance across all managed devices.

Browser Restart Enforcement: The patch only activates after Chrome restarts, so enforce or prompt a full browser restart on all endpoints. Verify that users have relaunched the application to load the patched binaries and fully mitigate the zero-day.

Interim Mitigation (If Patching Is Delayed): Disable WebGL or hardware acceleration to break the ANGLE exploit path, understanding this may affect graphics performance. Apply JavaScript restrictions in high-security units to reduce exposure to malicious web content that could deliver exploit triggers.

Monitoring and Incident Response: Actively watch for GPU process crashes, unexpected browser instability, or memory corruption indicators that may signal exploitation attempts. Investigate anomalies promptly and escalate to security teams if suspicious activity is detected.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0005 Defense Evasion
TA0004 Privilege Escalation	TA0006 Credential Access	T1203 Exploitation for Client Execution	T1555 Credentials from Password Stores
T1059.007 JavaScript	T1059 Command and Scripting Interpreter	T1211 Exploitation for Defense Evasion	T1555.003 Credentials from Web Browsers
T1068 Exploitation for Privilege Escalation	T1588.005 Exploits	T1588.006 Vulnerabilities	T1588 Obtain Capabilities
T1189 Drive-by Compromise	T1190 Exploit Public-Facing Application		

Patch Details

Upgrade Google Chrome to version 143.0.7499.109 (Linux) and 143.0.7499.109/.110 (Windows/macOS) or the latest available version.

Links:
https://www.google.com/intl/en/chrome/?standalone=1

https://chromereleases.googleblog.com/2025/12/stable-channel-update-for-desktop_10.html

References

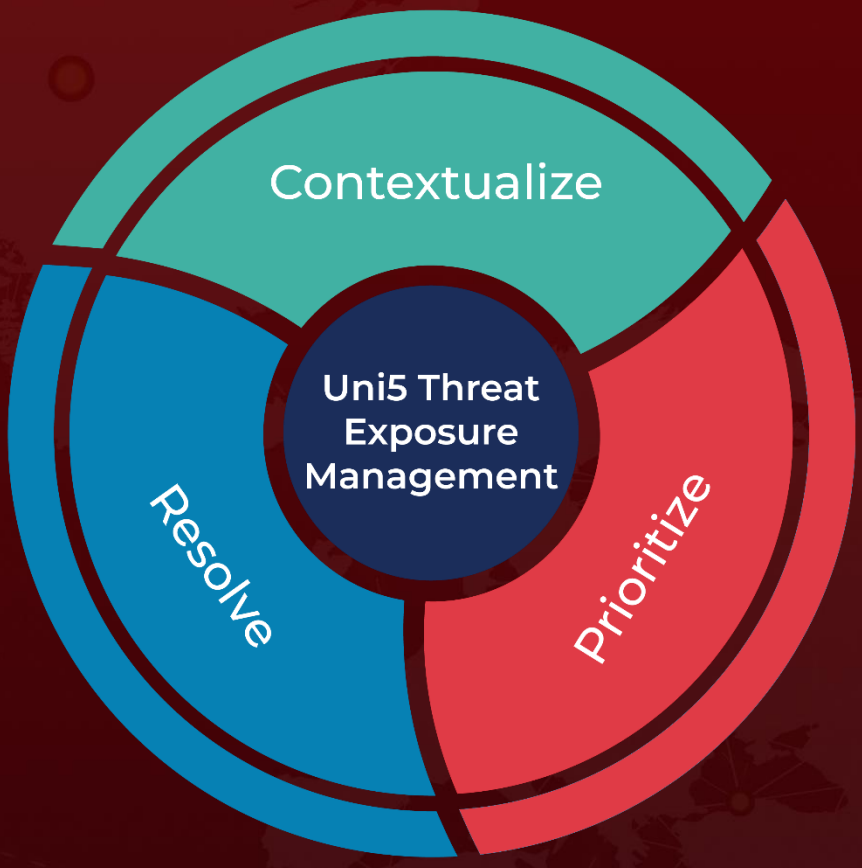
https://chromereleases.googleblog.com/2025/12/stable-channel-update-for-desktop_10.html

https://issues.chromium.org/issues/466192044

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

December 12, 2025 • 3:30 AM

More at www.hivepro.com