Active Exploitation of Chrome Zero-Day in ANGLE Graphics Library

TL;DR

Google confirmed active exploitation of a high-severity Chrome vulnerability, CVE-2025-14174, caused by an out-of-bounds memory access flaw in the ANGLE graphics library. The issue is being exploited in the wild.

All users should update Chrome immediately, and organizations should track patch availability for Chromium-based browsers.

Overview

Google released a Stable Channel security update for Chrome after confirming active exploitation of CVE-2025-14174, a high-severity out-of-bounds memory access vulnerability in the ANGLE (Almost Native Graphics Layer Engine) graphics library. ANGLE translates graphics calls across platforms, including Apple's Metal framework, and improper buffer handling in this component allows memory to be accessed outside its intended boundaries.

Affected Products

- Google Chrome (prior to patched versions)
- Chromium-based browsers that depend on ANGLE, including:
  - Microsoft Edge
  - Brave
  - Opera
  - Vivaldi

***Note**: Downstream browsers may remain exposed until vendors release their own patched builds.*

When triggered during certain graphics operations, the flaw can corrupt memory within the Chrome process. This can lead to browser crashes or attacker-controlled code execution. Google confirmed that an exploit exists in the wild but initially limited technical details to reduce follow-on exploitation while patches were deployed. On December 12, Google formally tied the activity to CVE-2025-14174.

Because the vulnerability can be triggered through normal browsing activity, such as visiting a malicious or compromised website, it does not require authentication or elevated privileges, making it particularly useful as an initial access point for attackers. This vulnerability was already being exploited before most users had patches available.

Organizations that lag on browser patching leave users exposed even during routine browsing. Aspire recommends patching as soon as possible.

Aspire Protects

- **Patch** – Update Chrome immediately to:
  - Windows / macOS – 143.0.7499.109 or .110
  - Linux – 143.0.7499.109
- Restart the browser to complete installation.
- Monitor vendor advisories for Chromium-based browsers until equivalent fixes are released.
- Prioritize patching for users with access to sensitive systems or data.

TTPs

Initial Access

- Drive-by Compromise [T1189] – The attacker may have delivered the exploit through a malicious or compromised website. A user simply visiting the page with an unpatched Chrome browser could trigger the ANGLE out-of-bounds memory access during graphics processing.

Execution

- Exploitation for Client Execution [T1203] – The attacker may have exploited CVE-2025-14174 to execute attacker-controlled code within the Chrome browser process by abusing improper memory handling in the ANGLE graphics library.

Privilege Escalation

- Exploitation for Privilege Escalation [T1068] (conditional) – If the attacker successfully chained this browser exploit with a secondary vulnerability, they may have attempted to escape the browser sandbox or elevate privileges on the underlying system.

Defense Evasion

- Obfuscated Files or Information [T1027] (conditional) – The attacker may have used obfuscated exploit code or hidden payloads within web content to avoid detection while delivering the browser-based exploit.

IoCs

There are no known IoCs at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

Targeted Industries

The Chrome zero-day threatens any organization relying on Chromium-based browsers for daily operations.

- Government
- Education
- Energy
- Healthcare
- Retail
- Finance
- Technology
- Legal
- Manufacturing

Aspire's Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.

- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.

  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

Chrome Releases: Stable Channel Update for Desktop

Metal: Don't use pixelsDepthPitch to size buffers. · google/angle@95a32cb · GitHub

GitHub - google/angle: A conformant OpenGL ES implementation for Windows, Mac, Linux, iOS and Android.