Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

CVE-2025-4664: Google Chrome’s Zero-Day Flaw Exploited in the Wild

Date of Publication	Admiralty Code	TA Number
May 16, 2025	A1	TA2025152

Summary

First Seen: May 5, 2025
Affected Product: Google Chrome, Microsoft Edge and other Chromium-based browsers
Impact: CVE-2025-4664 is a medium-severity zero-day vulnerability in Google Chrome's Loader component, allowing attackers to leak cross-origin data via crafted HTML pages. It exploits Chrome's handling of the Link header to set an unsafe referrer policy, exposing sensitive query parameters like OAuth tokens. Exploitation requires user interaction, such as visiting a malicious site. Google confirmed active exploitation, and users are urged to update Chrome immediately.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-4664	Google Chromium Loader Insufficient Policy Enforcement Vulnerability	Google Chromium, Microsoft Edge	✓	✓	✓
CVE-2025-4609	Google Chromium Mojo Sandbox Escape Vulnerability	Google Chromium, Microsoft Edge	✗	✗	✓

Vulnerability Details

#1

CVE-2025-4664 is a medium-severity (CVSS v3.1 score: 4.3) zero-day vulnerability in Google Chrome's Loader component, resulting from insufficient policy enforcement when handling subresource requests. This flaw allows attackers to leak cross-origin data by exploiting Chrome's unique behavior of resolving the Link header on subresource requests. Specifically, attackers can set an unsafe referrer policy (such as unsafe-url) via a crafted HTML page, causing sensitive query parameters—like OAuth tokens or session identifiers—to be sent to a domain they control.

#2 Exploitation of CVE-2025-4664 requires user interaction, typically in the form of convincing a victim to visit a specially crafted malicious web page. Once the user visits this page, the attacker's code can trigger cross-origin requests and collect sensitive data from the referrer, which would not be exposed under normal policy enforcement. This means the attack is not fully automatic; some form of social engineering or phishing is necessary to lure the user to the malicious site.

#3 The vulnerability affects Chrome versions prior to 136.0.7103.113 (Windows/Linux) and 136.0.7103.114 (macOS), and may also impact other Chromium-based browsers such as Microsoft Edge, Brave, and Opera until they are updated. Google has confirmed that this vulnerability has been exploited in the wild, underlining its seriousness. The main risk is the exposure of sensitive cross-origin data, which could lead to account compromise or unauthorized access if attackers obtain authentication tokens or session information.

#4 As part of the same security advisory, Google also addressed another issue tracked as CVE-2025-4609, which stems from an incorrect handle being provided in unspecified conditions within Mojo, a core IPC system in Chrome. Earlier, in March 2025, Google patched CVE-2025-2783, a high-severity Chrome zero-day exploited in "Operation ForumTroll" to deploy malware via phishing emails targeting Russian government, media, and educational institutions. Users are strongly advised to update their browsers to the latest versions to mitigate these vulnerabilities.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-4664	Google Chrome V8 prior to 136.0.7103.113 Microsoft Edge Version prior to 136.0.3240.76	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:* cpe:2.3:a:microsoft:edge:*:*:*:*:*:*:*:*	CWE-346
CVE-2025-4609	Google Chrome V8 prior to 136.0.7103.113 Microsoft Edge Version prior to 136.0.3240.76	cpe:2.3:a:ivanti:endpoint_manager_mobile:*:*:*:*:*:*:*:*	CWE-20

Recommendations

Update Browsers Immediately: Ensure that Google Chrome is updated to version 136.0.7103.113/.114 or later on Windows/Mac, and 136.0.7103.113 or later on Linux. For other Chromium-based browsers like Microsoft Edge, Brave, and Opera, apply the latest available patches as soon as they are released. Keeping browsers up to date is crucial to protect against known vulnerabilities.

Implement Secure HTTP Headers: Configure your web server to use a strict referrer policy, such as strict-origin-when-cross-origin, to limit the amount of referrer information sent with requests. Implement a robust Content Security Policy (CSP) to control the sources from which content can be loaded, reducing the risk of malicious content execution.

Audit and Secure Third-Party Resources: Regularly audit third-party scripts and resources included in your web applications to ensure they are from trusted sources. Use SRI to verify that resources hosted on third-party servers have not been tampered with.

Enhance Browser Security: Use enterprise-grade browser security tools to strengthen sandboxing and prevent attackers from bypassing isolation layers. Implement behavioral-based monitoring to detect unusual browser activity, such as unauthorized privilege escalations or unexpected process injections.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0004 Privilege Escalation
TA0006 Credential Access	T1588 Obtain Capabilities	T1588.005 Exploits	T1204 User Execution
T1528 Steal Application Access Token	T1190 Exploit Public-Facing Application	T1189 Drive-by Compromise	T1588.006 Vulnerabilities

Patch Details

- Upgrade Google Chrome version to 136.0.7103.113/.114 (Windows/Mac) and 136.0.7103.113 (Linux).
- Upgrade Microsoft Edge version to 136.0.3240.76.

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

https://www.microsoft.com/en-us/edge/download?form=MA13FW

References

https://chromereleases.googleblog.com/2025/05/stable-channel-update-for-desktop_14.html

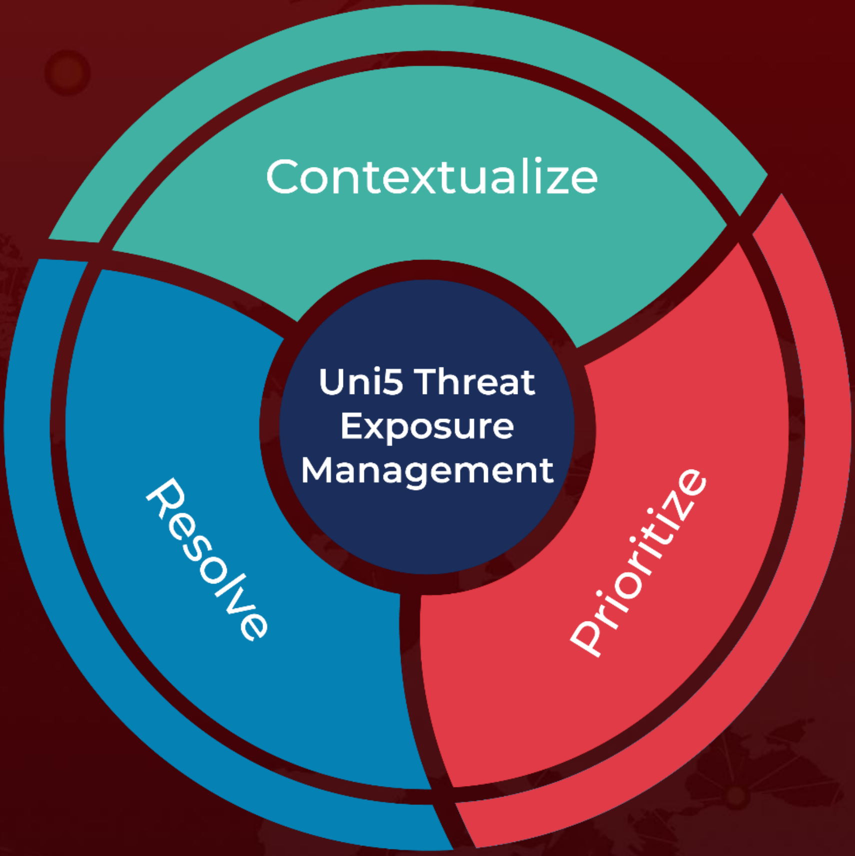
https://x.com/slonser_/status/1919439384811626706

https://hivepro.com/threat-advisory/chrome-zero-day-exploited-in-operation-forumtroll/

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

May 16, 2025 • 5:30 AM

More at www.hivepro.com