Chrome Referrer Policy Flaw Allows Cross-Origin Data Leak

Overview

Google released an update for Chrome to fix CVE-2025-4664(CVSS 4.3), a high-severity flaw that allows a remote attacker to leak cross-origin data, such as query parameters used in login and authorization flows. The issue stems from Chrome's behavior of processing Link headers on subresource requests, where a malicious page can set a permissive referrer policy (unsafe-url) and trick the browser into exposing private data.

An attacker could embed a third-party image or script in a malicious HTML page that forces Chrome to send referrer information from other origins, potentially leaking sensitive URL parameters to an external domain.

TL;DR

Google patched a high-severity Chrome vulnerability (CVE-2025-4664) that could let attackers steal sensitive information from other sites through crafted HTML pages. The bug has a public exploit and is being tracked as exploited in the wild.

Patch is now available for Chrome users on Windows, macOS, and Linux. Chromium-based browsers like Edge and Brave may also be affected.

Affected Versions

- Chrome (Stable Channel)
  - Windows/Linux: 136.0.7103.113
  - macOS: 136.0.7103.114
- Other Chromium-Based Browsers
  - Users of Microsoft Edge, Brave, Opera, and Vivaldi should watch for updates and apply them as soon as they're available.

This type of leak can have real consequences, especially when query strings contain session tokens, OAuth data, or other identifiers that aren't meant to be shared across sites. While it's not confirmed if this bug has been exploited for malicious purposes, the existence of a working exploit in the wild, and CISA adding it to its KEV catalog, means this is a real risk. Aspire recommends updating immediately.

Aspire Protects

- **Patch –** Ensure Chrome is updated to version 136.0.7103.113+ (Windows/Linux) or .114 (macOS).
- Instruct users to restart Chrome to complete the update if auto-updates are enabled.
- Monitor Chromium-based browsers and apply patches as they are released.
- Review any apps or services that include sensitive tokens in query parameters and adjust how session or auth data is passed.
- Stay alert for phishing attempts that may try to exploit this flaw via crafted links or embedded content.

TTPs to Watch

Collection

- Data from Information Repositories [T1213.001] – The attacker may have used referrer-policy manipulation to capture URL parameters containing sensitive data.

Exfiltration

- Exfiltration Over Command-and-Control Channel [T1041] – Captured data could be sent to third-party servers via embedded image or script tags.

Initial Access

- Drive-by Compromise [T1189] – Victims could be exposed simply by visiting a malicious site hosting the crafted HTML page.

IoCs

There are no known IoCs associated with the above vulnerability 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

This vulnerability affects anyone using Chrome or Chromium-based browsers, but it's especially relevant to industries that handle sensitive user data in web-based workflows, particularly those relying on OAuth, SSO, or token-based authentication.

- Healthcare
- Education
- Retail
- Finance
- Legal and Professional Services
- SaaS Providers

Aspire 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

NVD - CVE-2025-4664