

# Chrome Vulnerability Could Allow Arbitrary Code Execution

## Overview

Google has released a security update for Chrome to address a vulnerability, CVE-2025-3066, that could allow a remote attacker to execute arbitrary code on affected systems.

### Affected Products

- Google Chrome for Windows, macOS, and Linux prior to version 135.0.7049.84/.85

CVE-2025-3066 is a high-severity (CVSS 8.8) use-after-free vulnerability in Google Chrome's Site Isolation component. The flaw occurs when memory is improperly handled after it's released, creating an opportunity for attackers to execute arbitrary code. If exploited, the vulnerability could allow an attacker to compromise a system if a user visits a specially crafted website.

Use-after-free bugs in web browsers are often attractive to attackers due to the widespread use of these applications and the potential for remote code execution. While there's no sign this flaw has been exploited yet, that could change quickly. Aspire recommends updating Chrome to the latest version.

## Aspire Protects

- **Patch** – Update Chrome to version 135.0.7049.84 (Linux) or 135.0.7049.84/.85 (Windows/macOS) immediately.
- Restart the browser after updating to ensure the patch is applied.

### TTPs to Watch

#### Execution

- Exploit for Client Execution [T1203] – The attacker may have exploited a vulnerability in the browser to execute arbitrary code on the victim's system.

#### Initial Access

- Drive-by Compromise [T1189] – The attacker may have tricked the user into visiting a malicious website that triggered the vulnerability.

### 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

The vulnerability may impact any organization using Chrome:

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

## 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-2025-3066](#)