

Google Chrome Security Update – Several Vulnerabilities Patched

Overview

Google has released an update for Google Chrome (version 129.0.6668.70/.71 for Windows and Mac, and version 129.0.6668.70 for Linux) that addresses multiple security vulnerabilities. This update is rolling out gradually over the coming days and includes five critical security fixes, some of which could allow for arbitrary code execution.

Several vulnerabilities have been patched in this update and are rated as **High** severity:

- **CVE-2024-9120** - Use after free in Dawn
- **CVE-2024-9121** - Inappropriate implementation in V8
- **CVE-2024-9122** - Type Confusion in V8
- **CVE-2024-9123** - Integer overflow in Skia

Successful exploitation of these vulnerabilities could allow an attacker to execute arbitrary code within the context of the logged-on user. Depending on the user's privileges, this could allow an attacker to install programs, modify data, or create new accounts with full user rights. Although these vulnerabilities have not been exploited, Aspire recommends users make sure their Google Chrome browsers are updated as soon as possible.

Aspire Protects

- Apple is known to withhold security details until a majority of users are updated with a fix. They will also restrict information if the vulnerability is in a third-party library that other projects depend on but have not fixed.
- Apply the latest Google Chrome update immediately after testing to ensure security fixes are applied. To check for a Google Chrome update, please see below:
 - On your computer, open Chrome.
 - At the top right, click More .
 - Click Help and then About Google Chrome.
 - The current version number is the series of numbers beneath the "Google Chrome" heading. Chrome will check for updates when you're on this page.
 - To apply any available updates, click Relaunch.
- See below on how to update your Google Chrome browser:
 - On your computer, open Chrome.
 - At the top right, click More
 - Click Help. About Google Chrome

- Click Update Google Chrome. Important: If you can't find this button, you're on the latest version
- Click Relaunch
- Normally updates happen in the background when you close and reopen your computer's browser. But if you haven't closed your browser in a while, you might find a pending update:
 - On your computer, open Chrome.
 - At the top right, select More
 - If an update is pending, you'll find:
 - "Relaunch to update"
 - "Finish update"
 - "New Chrome available"
- For updates regarding these vulnerabilities, please see [Google's advisory](#).

IoCs

There are no known IoCs for the above vulnerabilities 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.

TTPs to Watch

- **Tactic: Initial Access (TA0001)**
 - Drive-By Compromise (T1189) – Attackers could execute arbitrary code when users visit a malicious or compromised website, leading to full system compromise if the user has administrative privileges.

Aspire's Service Offerings

- **Aspire Managed Security Services**
 - [Aspire Managed Security Services](#) provide remote security monitoring and device management – 24 hours a day, 7 days a week. By aggregating and correlating security events from across your IT environment, our remote security monitoring service eliminates “noise” and make sense of what really matters.
 - Our managed security portfolio includes:
 - Managed Firewall
 - Managed IDS/IPS
 - Security event monitoring & incident management
 - Managed Cisco ISE (Identity Services Engine)
 - Endpoint Protection



- **Aspire Managed Detection and Response (MDR)**
 - Accelerate the maturity of your security operations and reduce risk with faster threat detection and response capabilities. Aspire [MDR](#) delivers around-the-clock protection across cloud, network, and endpoints in one integrated solution.

Supporting Documentation

[Chrome Releases: Stable Channel Update for Desktop \(googleblog.com\)](#)

[Update Google Chrome - Computer - Google Chrome Help](#)