

HiveForce Labs

# THREAT ADVISORY

 **VULNERABILITY REPORT**

## Google Chrome Fixes Zero-Day CVE-2024-4671 Exploited in the Wild

Date of Publication

May 10, 2024

Admiralty Code

A1

TA Number

TA2024181

# Summary

**First Seen:** May 7, 2024

**Affected Product:** Google Chromium

**Impact:** The vulnerability in Google Chrome's Visuals component, identified as CVE-2024-4671, has been patched by Google in a recent security update. Exploitation could grant attackers remote code execution, prompting users to update to versions 124.0.6367.201/.202 for Windows and Mac, or 124.0.6367.201 for Linux, to safeguard against potential risks.

## ⚙️ CVE

| CVE           | NAME                                                 | AFFECTED PRODUCT | ZERO -DAY | CISA KEV | PATCH |
|---------------|------------------------------------------------------|------------------|-----------|----------|-------|
| CVE-2024-4671 | Google Chromium Visuals Use After Free Vulnerability | Google Chromium  | ✓         | ✓        | ✓     |

# Vulnerability Details

## #1

Google has issued a security update for Chrome, addressing the fifth zero-day vulnerability detected in 2024. Tracked as CVE-2024-4671, this high-severity flaw is in the Visuals component. It is a "use-after-free" vulnerability, which means that malicious code could attempt to use memory that has already been freed by the program. Depending on the user's privileges, this could lead to program installation, data manipulation, or creation of new accounts with full user rights.

## #2

This vulnerability has been observed being exploited in the wild. Systems running Chrome versions prior to 124.0.6367.201/.202 for Windows and Mac, and 124.0.6367.201 for Linux are at risk. Users are advised to apply the update manually if automatic updating is disabled or to restart the browser if prompted by a pending update notification. Other zero-day vulnerabilities patched by Google earlier in the year include [CVE-2024-3159](#), [CVE-2024-2887](#), [CVE-2024-2886](#), and [CVE-2024-0159](#).

# Vulnerabilities

| CVE ID        | AFFECTED PRODUCTS                     | AFFECTED CPE                            | CWE ID  |
|---------------|---------------------------------------|-----------------------------------------|---------|
| CVE-2024-4671 | Google Chrome prior to 124.0.6367.201 | cpe:2.3:a:google:chrome<br>:*:*:*:*:*:* | CWE-416 |

## Recommendations



**Update Chrome Immediately:** Ensure that all systems running Google Chrome are updated to version 124.0.6367.201/.202 for Windows and Mac, or 124.0.6367.201 for Linux. Promptly apply any security updates released by Google to stay protected against known vulnerabilities.



**Enable Automatic Updates:** Configure Chrome to automatically install updates to ensure that security patches are applied as soon as they become available, reducing the window of exposure to potential threats.



**Implement Web Filtering:** Employ web filtering solutions or browser extensions that can help block access to potentially malicious websites known for distributing malware or exploiting vulnerabilities.



**Implement Least Privilege:** Limit user privileges to the minimum necessary for performing their tasks. This can help mitigate the impact of potential exploits by restricting the ability of attackers to execute arbitrary code, install programs, or manipulate data.



**Vulnerability Scanning:** Conduct regular vulnerability scans on your network to identify any potential weaknesses or unpatched software. This proactive approach allows you to address security issues promptly before they can be exploited by attackers.

# Potential MITRE ATT&CK TTPs

|                                            |                                              |                                                              |                                                          |
|--------------------------------------------|----------------------------------------------|--------------------------------------------------------------|----------------------------------------------------------|
| <b><u>TA0002</u></b><br>Execution          | <b><u>TA0004</u></b><br>Privilege Escalation | <b><u>TA0042</u></b><br>Resource Development                 | <b><u>TA0001</u></b><br>Initial Access                   |
| <b><u>T1588</u></b><br>Obtain Capabilities | <b><u>T1588.006</u></b><br>Vulnerabilities   | <b><u>T1068</u></b><br>Exploitation for Privilege Escalation | <b><u>T1203</u></b><br>Exploitation for Client Execution |
| <b><u>T1588.005</u></b><br>Exploits        | <b><u>T1189</u></b><br>Drive-by Compromise   |                                                              |                                                          |

## Patch Details

Update Chrome browser to the latest version 124.0.6367.201/.202 for Mac and Windows and 124.0.6367.201 for Linux.

Link:

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

## References

[https://chromereleases.googleblog.com/2024/05/stable-channel-update-for-desktop\\_9.html](https://chromereleases.googleblog.com/2024/05/stable-channel-update-for-desktop_9.html)

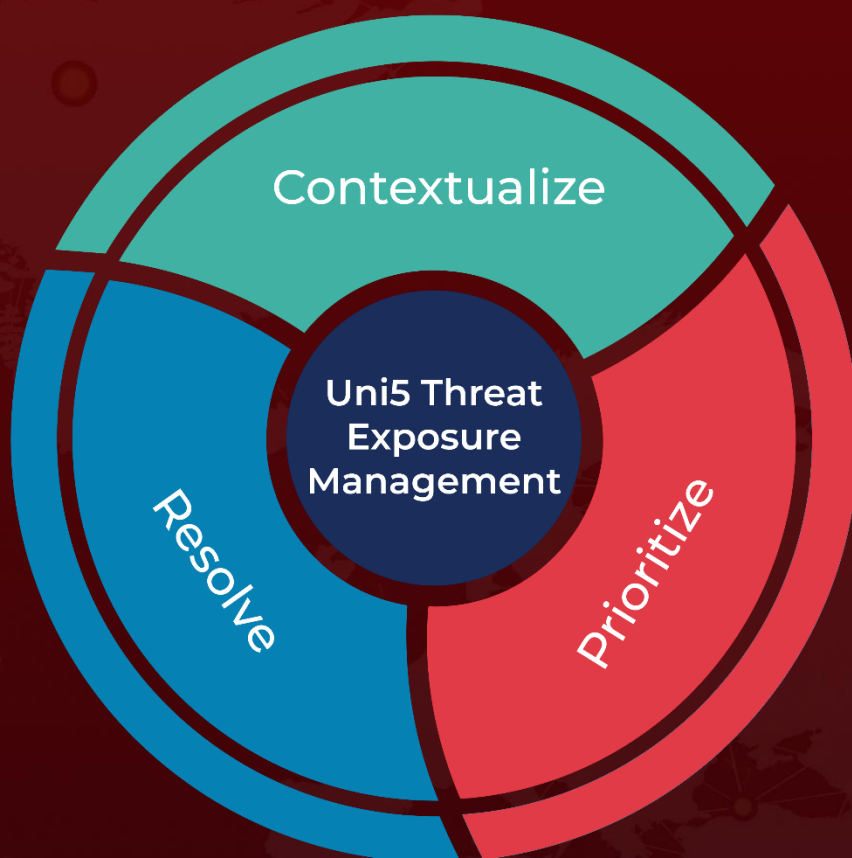
<https://www.hivepro.com/threat-advisory/google-patches-critical-zero-day-exploits-found-at-pwn2own/>

<https://www.hivepro.com/threat-advisory/google-fixes-first-actively-exploited-chrome-zero-day-of-2024/>

# 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 10, 2024 • 5:30 AM**

© 2024 All Rights are Reserved by Hive Pro



More at [www.hivepro.com](http://www.hivepro.com)