

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

Google Rushes to Fix Chrome Zero-Day Vulnerability

Date of Publication

June 3, 2025

Admiralty Code

A1

TA Number

TA2025170

Summary

First Seen: May 28, 2025

Affected Products: Google Chrome, Microsoft Edge and other Chromium-based browsers

Affected Platforms: Windows, macOS, and Linux

Impact: Google has patched a zero-day vulnerability (CVE-2025-5419) in Chrome's V8 engine that hackers are already abusing to attack unsuspecting users. The flaw lets malicious websites corrupt memory and potentially hijack your device; all it takes is visiting a crafted webpage. Chrome users on Windows, macOS, and Linux are strongly urged to update immediately to stay protected.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-5419	Google Chromium V8 Out-of-Bounds Read and Write Vulnerability	Google Chrome, Microsoft Edge			

Vulnerability Details

#1

Google has rolled out an urgent security update for its Chrome browser to fix a zero-day vulnerability that is already being exploited in the wild. The flaw, identified as CVE-2025-5419, is classified as high severity and involves out-of-bounds read and write access within Chrome's V8 JavaScript engine.

#2

The vulnerability could allow a remote attacker to corrupt memory by tricking users into visiting a specially crafted HTML page. This could potentially lead to heap corruption, opening the door to further exploitation, such as unauthorized code execution or system compromise. The issue affects all versions of Chrome prior to 137.0.7151.68.

#3

Demonstrating the seriousness of the threat, Google responded swiftly deploying a configuration change to the browser's stable channel just a day after identifying the issue. The fix is now available across all supported platforms, including Windows, macOS, and Linux.

#4

Google has confirmed that CVE-2025-5419 is being actively exploited in the wild. Users are strongly advised to update Chrome to the latest version without delay to safeguard their systems against potential attacks.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-5419	Google Chrome prior to 137.0.7151.68 Microsoft Edge	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:* cpe:2.3:a:microsoft:edge:*:*:*:*:*:*:**	CWE-787

Recommendations



Update Chrome Immediately: Go to Settings > About Chrome this will automatically check for updates. Make sure you're running version 137.0.7151.68 or later. This update includes the fix for the critical vulnerability. Don't delay attackers are already exploiting this flaw in the wild.



Turn On Automatic Updates (if disabled): Keeping auto-updates enabled helps ensure you get vital patches as soon as they're released without having to remember.



Avoid Clicking Suspicious Links or Downloading Unknown Files: Since attackers can use malicious web pages to exploit this flaw, be extra cautious while browsing. Stick to trusted websites and sources.



Vulnerability Management: This involves regularly assessing and updating software to address known vulnerabilities. Maintain an inventory of software versions and security patches, and evaluate the security practices of third-party vendors, especially for critical applications and services.



Potential MITRE ATT&CK TTPs

<u>TA0042</u> Resource Development	<u>TA0001</u> Initial Access	<u>TA0002</u> Execution	<u>T1588</u> Obtain Capabilities
<u>T1588.006</u> Vulnerabilities	<u>T1190</u> Exploit Public-Facing Application	<u>T1566</u> Phishing	<u>T1059</u> Command and Scripting Interpreter

Patch Details

Update your Google Chrome to the latest version to address the flaw.

For Mac Upgrade to Version 137.0.7151.68/.69

For Windows Upgrade to Version 137.0.7151.68/.69

For Linux Upgrade to Version 137.0.7151.68

Link:

<https://chromereleases.googleblog.com/2025/06/stable-channel-update-for-desktop.html>

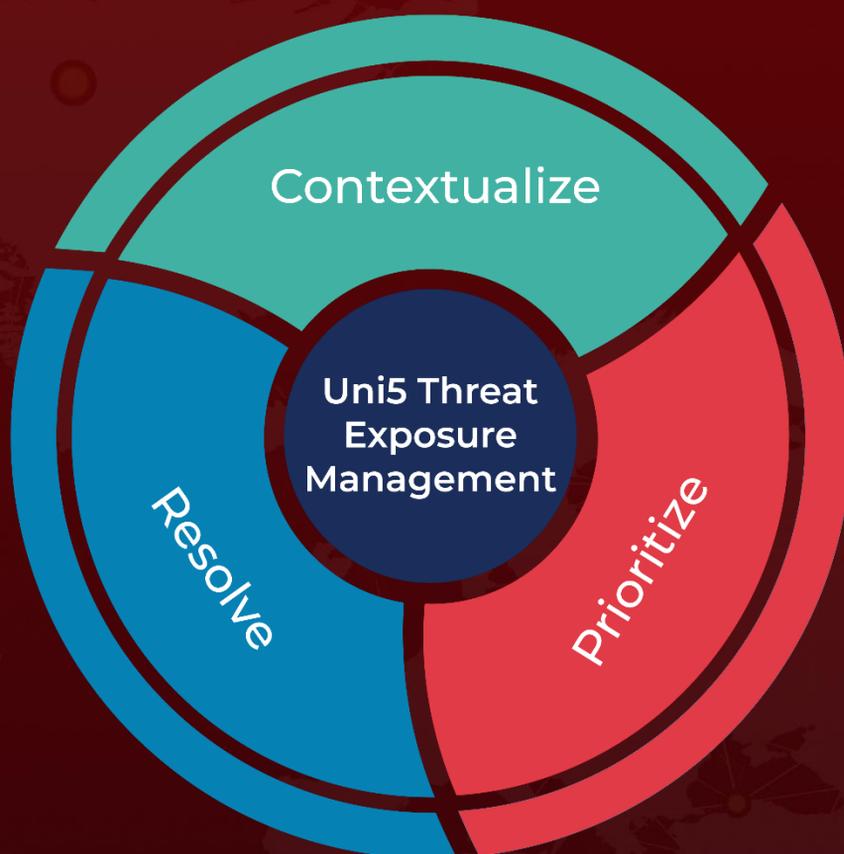
References

<https://chromereleases.googleblog.com/2025/06/stable-channel-update-for-desktop.html>

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

June 3, 2025 • 4:30 AM

© 2025 All Rights are Reserved by Hive Pro



More at www.hivepro.com