

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

CVE-2025-6558: Chrome Flaw Lets Hackers Break the Sandbox

Date of Publication

July 16, 2025

Admiralty Code

A1

TA Number

TA2025220

Summary

First Seen: June 23, 2025

Affected Product: Google Chrome

Impact: A zero-day flaw in Google Chrome (CVE-2025-6558) has been actively exploited in the wild, putting users at immediate risk. The issue stems from weak input validation in Chrome’s graphics components, allowing attackers to break out of the browser’s sandbox just by visiting a HTML page. Google responded quickly with an emergency patch (version 138.0.7204.157/.158), and users are strongly urged to update their browsers right away. Delaying the update could leave your system exposed to data theft, malware, or full compromise.

🔧 CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-6558	Google Chromium ANGLE and GPU Improper Input Validation Vulnerability	Google Chrome	✔️	✔️	✔️

Vulnerability Details

#1 A zero-day flaw in Google Chrome, tracked as CVE-2025-6558, has been uncovered, posing a significant risk to users. This high-severity vulnerability stems from insufficient validation of untrusted input in Chrome’s ANGLE and GPU components, which are responsible for handling graphics and rendering. In practical terms, a remote attacker could exploit this weakness through a specially crafted HTML page to break out of Chrome’s secure environment, an event known as a sandbox escape.

#2

The sandbox in Chrome is designed to act as a safety barrier, isolating web content from the rest of your operating system. But with CVE-2025-6558, attackers can bypass this crucial defense. If a user visits a malicious webpage, the flaw can allow harmful code to escape the browser's sandbox and execute directly on the victim's machine. This opens the door to a range of threats, everything from stealing sensitive data and installing spyware or ransomware to full system takeover.

#3

What makes this vulnerability especially concerning is that it was already being actively exploited in the wild before a patch was made available. Discovered and reported on June 23, 2025, Google responded quickly, issuing an emergency security update (version 138.0.7204.157/.158) on July 15, 2025.

#4

For all Chrome users, this is a critical warning: update your browser immediately. While Chrome usually updates in the background, it's essential to manually check and ensure you're on the latest version. Delaying this update could leave your system vulnerable to serious compromise. In a threat landscape where attackers move quickly, staying patched is your best defense.



Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-6558	Google Chrome prior to 138.0.7204.157	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*	CWE-20

Recommendations



Update Chrome Immediately: Go to your browser settings and manually check for updates. Install the latest version (138.0.7204.157 or .158). Don't wait for automatic updates, doing it now shuts the door on active attacks.



Restart Your Browser After Updating: Even if Chrome updates automatically in the background, it needs a restart to fully apply the fix. Make sure to close and reopen it.





Avoid Suspicious Websites: Until your browser is updated, avoid clicking on unknown links or visiting unfamiliar websites, as attackers could exploit the bug through a specially crafted page.



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>TA0005</u> Defense Evasion
<u>T1588</u> Obtain Capabilities	<u>T1588.006</u> Vulnerabilities	<u>T1189</u> Drive-by Compromise	<u>T1497</u> Virtualization/Sandbox Evasion
<u>T1204</u> User Execution			

Patch Details

Install the latest version of Google Chrome to address the flaw.
For Windows and Mac Update to Version 138.0.7204.157/.158
For Linux Update to Version 138.0.7204.157

Link:
https://chromereleases.googleblog.com/2025/07/stable-channel-update-for-desktop_15.html

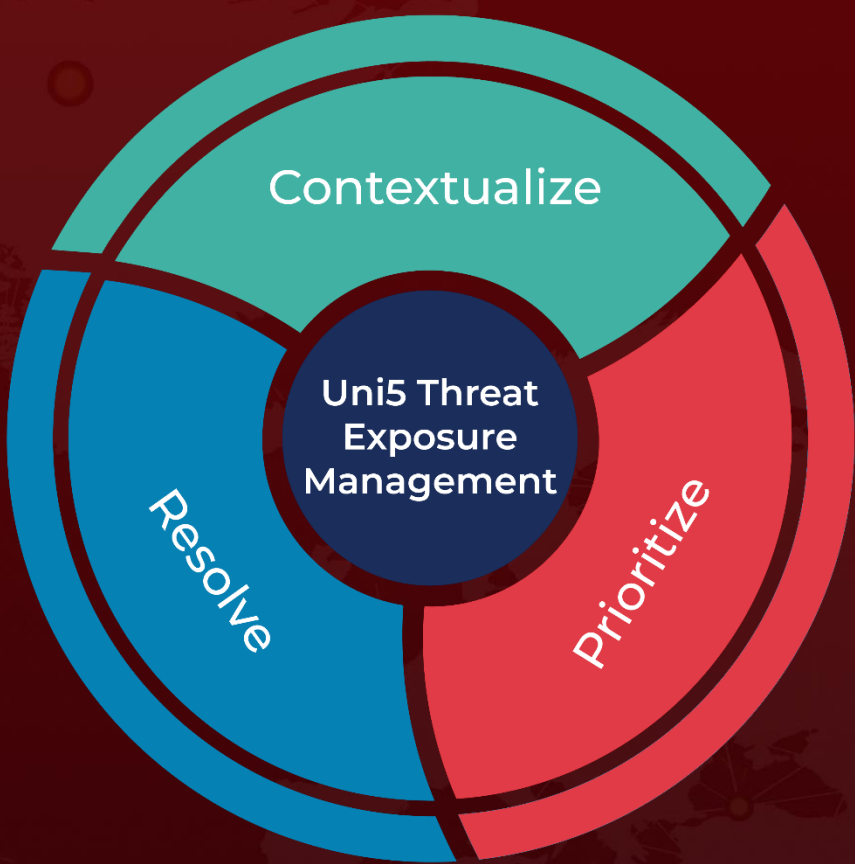
References

https://chromereleases.googleblog.com/2025/07/stable-channel-update-for-desktop_15.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
July 16, 2025 • 4:50 AM

