



THREAT ADVISORY

July 2, 2025

Chrome 0-Day Vulnerability Actively Exploited (CVE-2025-6554)

THREAT OVERVIEW

Google has confirmed active exploitation of a critical **0-day vulnerability (CVE-2025-6554)** in the Chrome browser. The flaw exists in Chrome's **V8 JavaScript engine** and enables **arbitrary code execution** through a type confusion error. Successful exploitation could allow attackers to take control of affected systems.

This vulnerability is already being exploited in the wild. Immediate action is required.

THREAT DETAILS

- **CVE ID:** CVE-2025-6554
- **Severity:** High
- **Exploit Status:** Actively exploited in the wild
- **Vulnerability Type:** Type Confusion in V8 (Chrome's JavaScript & WebAssembly engine)
- **Attack Impact:** Arbitrary code execution with browser-level privileges
- **Reported by:** Clément Lecigne, Google Threat Analysis Group
- **Discovery Date:** June 25, 2025
- **Initial Mitigation Deployed:** June 26, 2025
- **Patch Release Version:**
 - Windows: 138.0.7204.96/.97
 - Mac: 138.0.7204.92/.93
 - Linux: 138.0.7204.96

ATTACK VECTOR

1. Exploitation may occur via:
 - Malicious websites that trigger the vulnerability when visited
 - Compromised web applications or advertisements
 - Drive-by download attacks via social engineering or phishing campaigns
2. This is a **client-side vulnerability**, meaning end-user browsers are the attack surface.

IMMEDIATE ACTIONS – FOR INDIVIDUALS & END USERS

1. **Update Chrome Immediately**
 - a. Navigate to: Settings > About Chrome
 - b. Chrome will auto-check for updates and prompt for a restart.
 - c. Ensure version matches or exceeds the fixed release.
2. **Restart Chrome** after the update to apply the patch.
3. **Avoid Untrusted Links or Suspicious Sites** until your browser is patched.

REMEDIATION – FOR SECURITY TEAMS / IT ADMINISTRATORS

1. **Force Update Across Fleet**
 - Use enterprise device management tools (e.g., GPO, Intune, Jamf) to enforce Chrome updates.
 - Validate Chrome version deployment across Windows, macOS, and Linux endpoints.
2. **Monitor for Indicators of Exploitation**
 - Audit outbound traffic for unusual domains.
 - Review endpoint alerts tied to browser behavior, memory access, or script anomalies.
 - Enable/verify EDR solutions are active on all Chrome-using endpoints.
3. **Communicate Internally**
 - Send an internal security bulletin to employees explaining the update urgency.
 - Require browser updates prior to accessing sensitive systems, if feasible.
4. **Strengthen Browser Isolation Policies**
 - Use tools like Chrome Enterprise's site isolation features.
 - Consider sandboxing Chrome usage for high-risk users or privileged roles.

STRATEGIC RECOMMENDATIONS

- **Implement Auto-Update Enforcement** for all browsers in your environment.
- **Leverage Threat Intelligence Feeds** to monitor for CVE-2025-6554 exploitation campaigns.
- **Conduct a Rapid Patch Validation Audit** across all user endpoints this week.
- For SMBs lacking internal cybersecurity resources, consider engaging a managed security service provider (MSSP) like **Blackswan Cybersecurity**, who can help assess exposure and implement critical patch compliance monitoring through services like **Active Incident Exposure (AIE)**.

CONCLUSION

This vulnerability underscores the risk of unpatched software—even in widely trusted platforms like Chrome. With **active exploitation confirmed**, this is not a theoretical risk. IT leaders must act swiftly to patch systems, verify coverage, and monitor for abuse.

The speed of Google's response is commendable, but protection ultimately depends on **user and enterprise action**.

To learn more or to discuss your security posture, [contact us](#) at: contact@blackswancybersecurity.com or blackswan-cybersecurity.com.

REFERENCES

- <https://thehackernews.com/2025/07/google-patches-critical-zero-day-flaw.html>
- <https://cybersecuritynews.com/chrome-0-day-vulnerability-exploited/>