Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Chrome Zero-Day Exploited in Operation ForumTroll

Date of Publication	Admiralty Code	TA Number
March 26, 2025	A1	TA2025095

Summary

First Seen: March 20, 2025
Affected Products: Google Chrome (Windows)
Targeted Country: Russia
Targeted Industries: Media Outlets, Educational Institutions and Government Organizations
Campaign: Operation ForumTroll
Impact: Google has addressed a high-severity vulnerability in Chrome on Windows, that hackers have actively exploited in the wild. Tracked as CVE-2025-2783, the flaw stems from an incorrect handle being provided in certain unspecified conditions within Mojo, Chrome's IPC framework. While technical details remain limited, attackers have used this flaw to target organizations in Russia, highlighting its real-world impact. It is being weaponized in phishing attacks, redirecting victims to a malicious domain as part of a cyber-espionage campaign known as Operation ForumTroll.

⚙ CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-2783	Google Chromium Mojo Sandbox Escape Vulnerability	Google Chrome (Windows)	✓	✓	✓

Vulnerability Details

#1 Google has released a critical security update for Chrome on Windows, addressing a high-severity zero-day vulnerability actively exploited in targeted attacks. Tracked as CVE-2025-2783, the flaw arises from an incorrect handle being provided under unspecified conditions within Mojo, Chrome's IPC framework. Threat actors leveraged this weakness to infiltrate Russian organizations.

#2 What makes CVE-2025-2783 particularly alarming is its ability to bypass Chrome's sandbox protections effortlessly, as if they didn't exist. This was not achieved through a traditional exploit chain but rather through a logical flaw at the intersection of Chrome's sandbox and the Windows OS itself. The attackers skillfully took advantage of this weakness to execute code outside of Chrome's secure environment, gaining deeper access to compromised systems.

#3 The attack, dubbed Operation ForumTroll, showcases a sophisticated and state-sponsored approach. Victims were lured in through phishing emails disguised as invitations to the "Primakov Readings" forum, a well-known academic and policy event. The emails primarily targeted media outlets, educational institutions, and government bodies in Russia, tricking recipients into clicking malicious links. Once opened in Chrome, the exploit was triggered immediately, allowing attackers to gain initial access without raising red flags.

#4 Given the severity of the flaw and its active exploitation, users are strongly advised to update Chrome immediately to protect against potential threats. This attack underscores the evolving nature of zero-day exploitation, where even well-secured environments can be breached through subtle yet powerful vulnerabilities.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-2783	Google Chrome (Windows) Version Prior to 134.0.6998.178	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	CWE-20

Recommendations

Upgrade Immediately : Update your Google Chrome to the latest version to patch CVE-2025-2783. Enable automatic updates to stay protected against future zero-days.

Enhance Email Security: Use advanced email filtering tools to catch and block phishing attempts before they reach inboxes. Educate employees on spotting tricky emails, like fake event invitations used in Operation ForumTroll, to prevent accidental clicks on malicious links.

Enhance Browser Security: Use enterprise-grade browser security tools to strengthen sandboxing and prevent attackers from bypassing isolation layers. Implement behavioral-based monitoring to detect unusual browser activity, such as unauthorized privilege escalations or unexpected process injections.

System-Level Security Controls: Restrict access to untrusted websites and use DNS filtering to block known malicious domains linked to phishing attacks. For high-risk environments, consider browser isolation to reduce exposure. Strengthen defenses with Application Control to block unauthorized code execution and deploy Endpoint Detection and Response (EDR) solutions for real-time threat monitoring.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0001** Initial Access	**TA0002** Execution	**TA0005** Defense Evasion
T1588 Obtain Capabilities	**T1588.006** Vulnerabilities	**T1566** Phishing	**T1497** Virtualization/Sandbox Evasion
T1059 Command and Scripting Interpreter	**T1036** Masquerading	**T1204** User Execution	

Indicator of Compromise (IOCs)

TYPE	VALUE
Domain	primakovreadings[.]info

Patch Details

To safeguard against the CVE-2025-2783 vulnerability, Update Chrome browser to the latest version 134.0.6998.178.

Link:
https://chromereleases.googleblog.com/2025/03/stable-channel-update-for-desktop_25.html

References

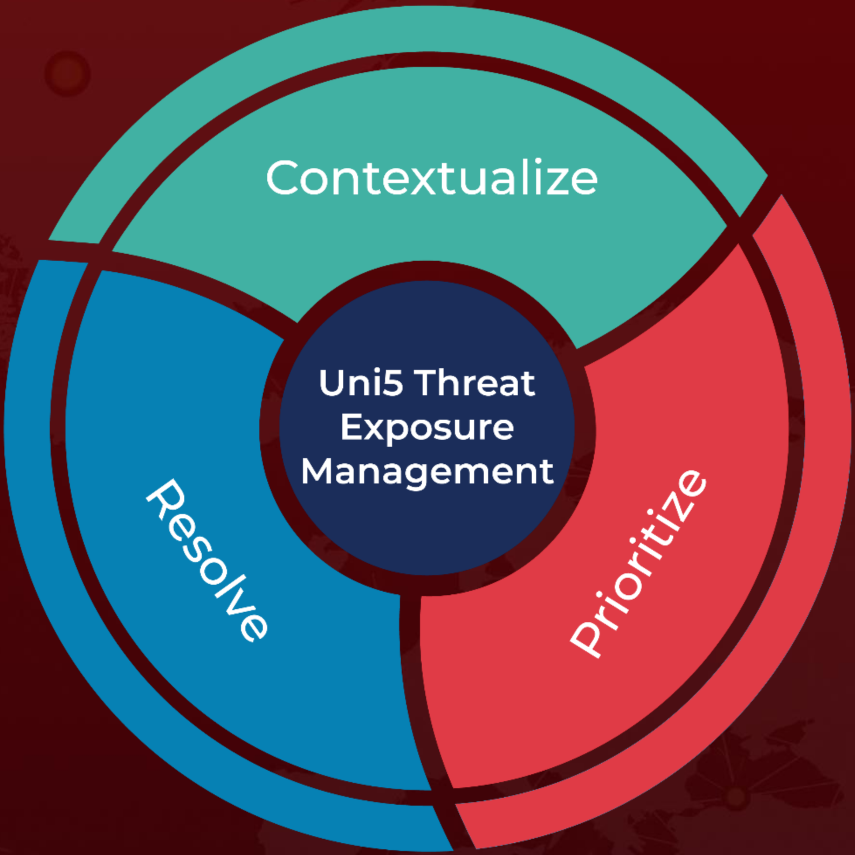
https://chromereleases.googleblog.com/2025/03/stable-channel-update-for-desktop_25.html

https://securelist.com/operation-forumtroll/115989/

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

March 26, 2025 • 4:20 AM

More at www.hivepro.com