Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Chrome Zero-Day Exploited in the Wild

Date of Publication	Last Update Date	Admiralty Code	TA Number
March 26, 2025	October 30, 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
Actor: TaxOff
Malware: Trinper, LeetAgent
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. 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 Operation ForumTroll began with highly targeted spear-phishing messages that lured victims into clicking a short-lived link. That single click executed a small "validator" script in the browser, which then handed off to a previously unknown Chromium sandbox-escape exploit, granting the attackers code execution from inside the browser. From that foothold, a compact and discreet loader was installed, creating Base64-named folders and modules to stay hidden. It then fetched LeetAgent, a suite of implants designed for real-time surveillance, including keystroke logging, screenshot capture, file harvesting, and selective data exfiltration. The campaign was surgical, using social engineering to gain entry, a stealthy browser exploit to break containment, a persistent loader to stage tools, and LeetAgent to conduct long-term espionage while blending into normal system activity.

#4 The campaign has been attributed to the TaxOff group, which deploys a malware strain known as Trinper. Written in C++, Trinper uses multithreading to gather host information, log keystrokes, and maintain a persistent connection with a remote server to receive commands and exfiltrate execution results. TaxOff is likely the same group known as Team46, based on overlaps in tactics, tools, and infrastructure. Users are strongly advised to update Google Chrome immediately to mitigate the risk of compromise.

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	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	TA0009 Collection
TA0010 Exfiltration	TA0011 Command and Control	T1588 Obtain Capabilities	T1588.006 Vulnerabilities
T1588.005 Exploits	T1566 Phishing	T1566.002 Spearphishing Link	T1059 Command and Scripting Interpreter
T1059.001 PowerShell	T1204 User Execution	T1204.001 Malicious Link	T1204.002 Malicious File
T1106 Native API	T1497 Virtualization/Sandbox Evasion	T1497.001 System Checks	T1055 Process Injection
T1055.012 Process Hollowing	T1027 Obfuscated Files or Information	T1041 Exfiltration Over C2 Channel	T1572 Protocol Tunneling

T1070 Indicator Removal	**T1070.004** File Deletion	**T1070.009** Clear Persistence	**T1480** Execution Guardrails
T1480.001 Environmental Keying	**T1036** Masquerading	**T1562** Impair Defenses	**T1562.001** Disable or Modify Tools
T1622 Debugger Evasion	**T1056** Input Capture	**T1056.001** Keylogging	**T1057** Process Discovery
T1083 File and Directory Discovery	**T1115** Clipboard Data	**T1071** Application Layer Protocol	**T1090** Proxy
T1090.004 Domain Fronting	**T1132** Data Encoding	**T1132.001** Standard Encoding	**T1573** Encrypted Channel
T1573.001 Symmetric Cryptography	**T1573.002** Asymmetric Cryptography	**T1082** System Information Discovery	

Indicator of Compromise (IOCs)

TYPE	VALUE
Domains	primakovreadings[.]info, mil-by[.]info, primakovreadings[.]info, 2025primakovreadings[.]info, primakovreadings2025[.]info, ads-stream-api-v2[.]global[.]ssl[.]fastly[.]net, fast-telemetry-api[.]global[.]ssl[.]fastly[.]net, browser-time-stats[.]global[.]ssl[.]fastly[.]net, rdp-query-api[.]global[.]ssl[.]fastly[.]net, rdp-statistics-api[.]global[.]ssl[.]fastly[.]net, clip-rdp-api[.]global[.]ssl[.]fastly[.]net, rdp-api-front[.]global[.]ssl[.]fastly[.]net, common-rdp-front[.]global[.]ssl[.]fastly[.]net, front-static-api[.]global[.]ssl[.]fastly[.]net, main-front-api[.]global[.]ssl[.]fastly[.]net, ms-appdata-fonts[.]global[.]ssl[.]fastly[.]net, ms-appdata-main[.]global[.]ssl[.]fastly[.]net, ms-appdata-query[.]global[.]ssl[.]fastly[.]net

TYPE	VALUE
MD5	7d3a30dbf4fd3edaf4dde35ccb5cf926, 07d2b50cf8ffe13a4722955ea94317aa, f3a70b8073ce2276af75b1cc2f18aced, 4b51f3021d8426b8356cd5751ad6ebd0, 16f6227f760487a70a3168cf9a497ac3, 1b7b4608f2c9e0a4863a00edd60c3b78, dba17d2faa311f28e68477ea5cc1a300, ca767542f4af58fc3072e74574725ee3, 5f47e40f3a36cc06bbaec27b063cd195, d69854b4a5c324082e157f04889ba138, d003e812336221db029f02738451215c, 33bb0678af6011481845d7ce9643cedc, 35869e8760928407d2789c7f115b7f83
SHA1	3650c1ac97bd5674e1e3bfa9b26008644edacfed, ff01b509d72662f1d0541d37fd89165d15ad8262, 197b98d7f368bfd5bd7210b5215a720b8dba83a1, 643966f0b58b2c1c9d7fead5f9d8b528ea76faaa, 20943541522cd3937b275c42016ad3e1e64e3f38, d9fa06025ecd08fc417c9948148e7827280365f2, 39ecc624bd2d52db083424fbb3a47b0c60f5ae4e, c1795c171d88cbf36e36fe2d3a3feb435e24c29a, 8a79060165774fc8d6cf099109a043f07476aa7a, 5dafc8e4ed184653b8cfb1769617b4e2e27168c3, f12d9b983d5bcc93d99b8199da84e8c4240caaa5, 8390e2ebdd0db5d1a950b2c9984a5f429805d48c, c25275228c6da54cf578fa72c9f49697e5309694
SHA256	2e39800df1cafbebfa22b437744d80f1b38111b471fa3eb42f2214a5ac7e1f13, f062681125a93a364618da3126c42b6e7c8f27910e954a7b8afd72455ddce328, b159534cd3bf2fa350edf18969ea4b07cb3cded49c40d927bac19ff390589504, ab42a3c6ff062147fa7bbf527f7b0b106c1514872bd1a90c8868423fa0485038, f15d8c58d8edb2ec17d35fe9d65062a767067760896eb425fc0de0d4536cc666, d622119cd68ad24f3498c54136242776d69ffe1f6b382a984616a667849c08b2, 99786a04acc05254dd35b511c4b3af34c88251f926c4ef91c215a9fce6ba8f96, fde9725923e15ca4f790c0ad4766fe7d60e6e3dae75ea8ccf04ff42f2458b4b1, 7975d287b07454b68455dd7e052eb741b5bf81712596ea00ddda2b103a99d037, 185cdfd1eeef2a4063e5134653c53058f91050de8c9234740a7ddd215a2aeaed,

TYPE	VALUE
SHA256	2997647affa42eff41a27c5db54b126087a36f789c8cfc66d24a21fe7212badc, 388a8af43039f5f16a0673a6e342fa6ae2402e63ba7569d20d9ba4894dc0ba59, 07d272b607f082305ce7b1987bfa17dc967ab45c8cd89699bcdced34ea94e126
IPv4	185[.]81[.]114[.]15
Filenames	twinapi.dll, winsta.dll, WINSTA.dll, AdobeARM.exe, dirlist.exe, ProcessList.exe, ScreenShot.exe

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/

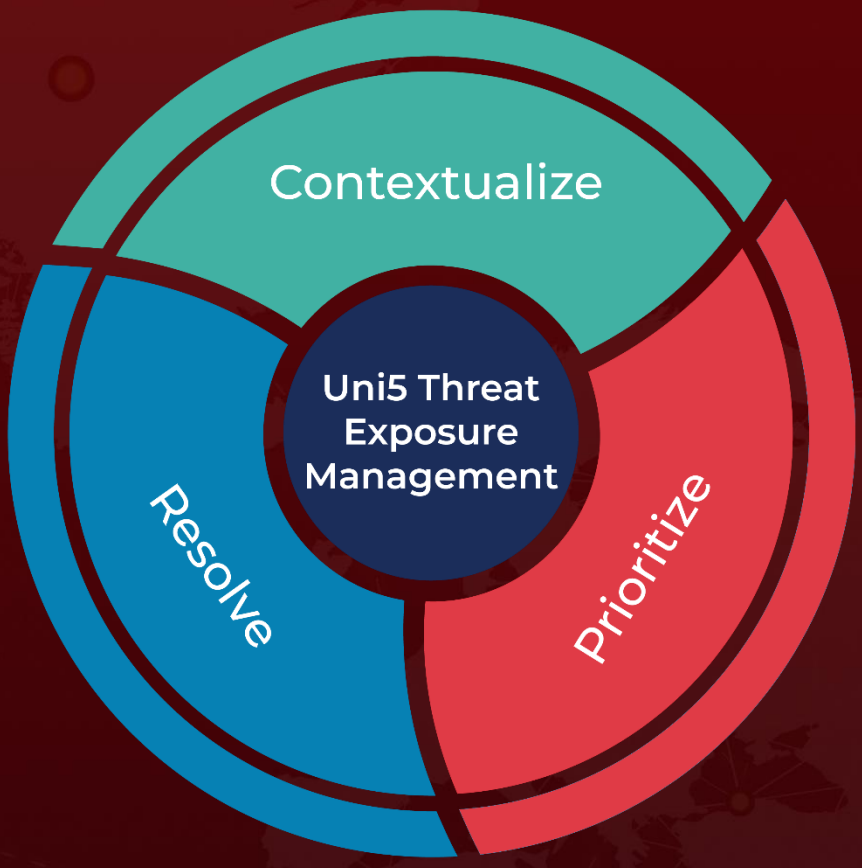
https://global.ptsecurity.com/analytics/pt-esc-threat-intelligence/team46-and-taxoff-two-sides-of-the-same-coin#Trinper%20loader

https://securelist.com/forumtroll-apt-hacking-team-dante-spyware/117851/

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