CVE-2025-2783

CHROME ZERO-DAY EXPLOIT

Vairav CVE Report

Date: March 26, 2025

Vairav Cyber Threat Intelligence Team

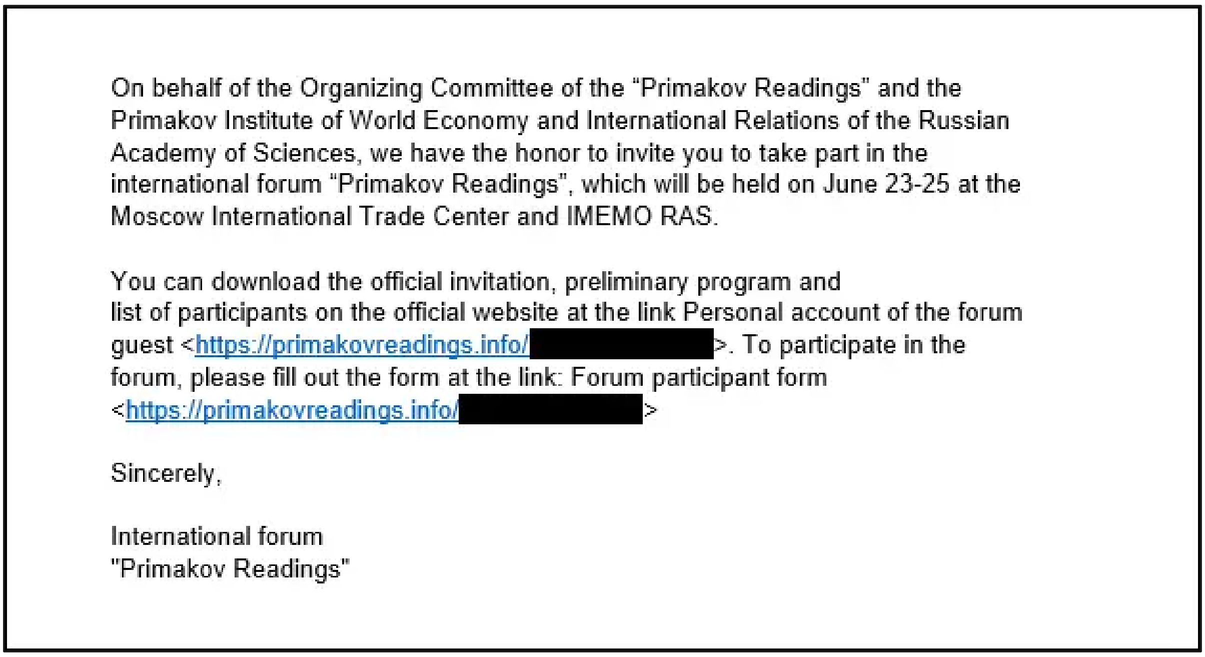
Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148
Baluwatar, Kathmandu

Phone: +977 4541540
Mobile: +977-9820105900
Email: sales@vairavtech.com

EXECUTIVE SUMMARY

Kaspersky Labs has uncovered a **Google Chrome zero-day exploit (CVE-2025-2783)** being actively used in a cyber-espionage campaign called **Operation ForumTroll**. Attackers exploited this vulnerability to bypass Chrome's sandbox protection, enabling remote code execution on targeted systems. The campaign, attributed to a state-sponsored APT group, used spear-phishing emails impersonating the Primakov Readings forum to lure victims into opening malicious links, triggering the exploit. Google has patched the vulnerability in **Chrome version 134.0.6998.177/.178** for Windows, and immediate updates are advised.



On behalf of the Organizing Committee of the "Primakov Readings" and the Primakov Institute of World Economy and International Relations of the Russian Academy of Sciences, we have the honor to invite you to take part in the international forum "Primakov Readings", which will be held on June 23-25 at the Moscow International Trade Center and IMEMO RAS.

You can download the official invitation, preliminary program and list of participants on the official website at the link Personal account of the forum guest <https://primakovreadings.info/[redacted]>. To participate in the forum, please fill out the form at the link: Forum participant form <https://primakovreadings.info/[redacted]>

Sincerely,

International forum
"Primakov Readings"

Figure 1: Example of a malicious email used in this campaign (translated from Russian)

VULNERABILITY DETAILS

CVE-2025-2783: Chrome Zero-Day Exploit

Description: This vulnerability in **Google Chrome's Mojo IPC (Inter-Process Communication)** allowed attackers to bypass Chrome's sandbox security, granting unauthorized access to the underlying system. Once exploited, attackers could execute arbitrary code without requiring user interaction beyond opening a malicious website.

Impact: Unauthorized sandbox escape, remote code execution (RCE), intelligence gathering.

CVSS Score: N/A (High)

AFFECTED VERSIONS

- Google Chrome versions before 134.0.6998.177/.178 on Windows

EXPLOIT DETAILS

- **Attack Vector:** Spear-phishing emails impersonating invitations to the Primakov Readings forum contained malicious links. Clicking the link triggered the silent exploitation of CVE-2025-2783, allowing malware to infiltrate the system.
- **Bypassing Chrome's Sandbox:** The exploit leveraged Mojo IPC manipulation to evade Chrome's security mechanisms, enabling unauthorized system access and potential remote code execution.
- **Indicators of Sophisticated Threat Actors:** The attackers used personalized emails, rapidly expiring malicious links, and second-stage exploits. RECOMMENDED ACTIONS

RECOMMENDATIONS

Patch & Upgrade:

- VMware Update Google Chrome to version 134.0.6998.177/.178 immediately to mitigate this vulnerability.
- Organizations should enforce automatic browser updates across all endpoints.

Mitigation Measures:

- Strengthen email filtering and link-tracking protections to prevent spear-phishing attacks.
- Educate users on phishing risks and advise against clicking unfamiliar links.
- Monitor logs for indicators of compromise (IOCs) associated with Operation ForumTroll.

REFERENCES

https://securityonline.info/cve-2025-2783-chrome-zero-day-exploited-in-state-sponsored-espionage-campaign/

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

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

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com