



CHROME BUFFER OVERFLOW VULNERABILITIES

Vairav Advisory Report

Date: February 19, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: mail@vairavtech.com

EXECUTIVE SUMMARY

Google has urgently patched two high-severity heap buffer overflow vulnerabilities (CVE-2025-0999 and CVE-2025-1426) in its Chrome browser. These vulnerabilities, affecting the V8 JavaScript engine and GPU components, respectively, allow attackers to execute arbitrary code and potentially take full control of affected systems. An additional medium-severity vulnerability (CVE-2025-1006) in Chrome's Network component has also been addressed. Users are advised to update Chrome immediately to mitigate risks.

VULNERABILITY DETAILS

CVE-2024-0999

Description: A heap buffer overflow vulnerability in Chrome's V8 JavaScript engine due to improper memory management when processing JavaScript objects. Attackers can exploit this flaw using crafted HTML pages to trigger heap corruption.

Impact: Remote Code Execution (RCE), system compromise

CVSS Score: High

CVE-2024-1426

Description: A heap buffer overflow vulnerability in Chrome's GPU component. Attackers can exploit buffer limit overflows during rendering operations to achieve code execution.

Impact: Remote Code Execution (RCE), potential full system compromise

CVSS Score: High

CVE-2024-1006

Description: A use-after-free (UAF) vulnerability in Chrome's Network component. Malicious web content can exploit this flaw to trigger arbitrary code execution or exfiltrate sensitive data.

Impact: Arbitrary code execution, data leakage

CVSS Score: Medium

AFFECTED VERSIONS

Google Chrome: Before 133.0.6943.126/.127 (Windows/Mac) and 133.0.6943.126 (Linux)
Fixed in 133.0.6943.126/.127 (Windows/Mac) and 133.0.6943.126 (Linux)

EXPLOIT DETAILS

Exploitation of these vulnerabilities could allow remote attackers to execute arbitrary code by crafting malicious web content, leading to full system compromise, data exfiltration, or lateral movement within a network. While no active exploitation has been confirmed, Google has withheld full technical details until most users update.

RECOMMENDED ACTIONS

- Users should update Chrome to the latest version via Chrome > Help > About Google Chrome and restart the browser.
- Enterprises should ensure timely deployment across networks to prevent exploitation.

ADDITIONAL SECURITY MEASURES

- Enforce browser security policies to prevent untrusted script execution.
- Enable site isolation and other security features within Chrome.
- Detect and block malicious web content leveraging Chrome vulnerabilities.

REFERENCES

<https://cybersecuritynews.com/chrome-buffer-overflow-vulnerabilities/>
https://chromereleases.googleblog.com/2025/02/stable-channel-update-for-desktop_18.html

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: mail@vairavtech.com

Website: <https://vairavtech.com>