



ESF LABS LIMITED

CYBER ADVISORY REPORT

GOOGLE PATCHES SEVERE VULNERABILITIES IN
CHROME | 9-3-2024



CYBER ADVISORY



EXECUTIVE SUMMARY

Google has released the stable channel updates to **128.0.6613.119/.120** for Windows, Mac and **128.0.6613.119** for Linux, which will roll out over the coming days/weeks. Total of 04 vulnerabilities were identified by the official vendor.

This advisory report briefs the readers about the vulnerabilities and the recommendations that needed to apply in the organization as well as for the individuals to be protected from such threats. Further technical detailing has been mentioned in this report.

TECHNICAL DETAILS

The vulnerabilities with details are mentioned below:

CVE ID	Vulnerability Name	Description	CVSS Score	Severity
CVE-2024-8362	Google Chrome code execution	Google Chrome could allow a remote attacker to execute arbitrary code on the system, caused by a use-after-free in WebAudio. By persuading a victim to visit a specially crafted Web site, a remote attacker could exploit this vulnerability to execute arbitrary code on the system.	8.8	High 
CVE-2024-7970	Google Chrome code execution	Google Chrome could allow a remote attacker to execute arbitrary code on the system, caused by an out-of-bounds write in V8. By persuading a victim to visit a specially crafted Web site, a remote attacker could exploit this vulnerability to execute arbitrary code on the system.	8.8	High 

Recommendation(s)	<ul style="list-style-type: none">• User are advised to upgrade to the latest version of Google Chrome 127.0.6533.99/.100 or later.• It is recommended for the Google Chrome users to update the browser to the latest version by visiting the official Google Chrome vendor's website and follow the following steps to update the patch.<ul style="list-style-type: none">○ Google Chrome users can go to chrome://settings/help by clicking Settings > About Chrome○ If an update is available Chrome will notify users and then start the download process○ Users can then relaunch the browser to complete the update.• Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.• User should not visit un-trusted websites or follow links provided by unknown or un-trusted sources.• Users should have knowledge regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.• Apply the Principle of Least Privilege to all systems and services.
Reference(s)	https://chromereleases.googleblog.com/