



مجلس الأمن السيبراني  
CYBER SECURITY COUNCIL



**Google Chrome OS Security Updates**

Tracking #:432315992

Date:27-06-2024

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLIGENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Google recently released security updates to address vulnerabilities in the Chrome OS.

## TECHNICAL DETAILS:

Google has released security updates to address vulnerabilities in Chrome OS.

### Vulnerability Details:

- **CVE-2024-5493 (High):** Heap buffer overflow in WebRTC-Heap buffer overflow in WebRTC in Google Chrome prior to 125.0.6422.141 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
- **CVE-2024-5496 (High):** Use after free in Media Session-Use after free in Media Session in Google Chrome prior to 125.0.6422.141 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.

### Fixed Versions:

- LTS-120 is being updated in the LTS (Long Term Support) channel, version 120.0.6099.315 (Platform Version: 15662.112)

## RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the security updates recently released by Google.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

## REFERENCES:

- [https://chromereleases.googleblog.com/2024/06/long-term-support-channel-update-for\\_26.html](https://chromereleases.googleblog.com/2024/06/long-term-support-channel-update-for_26.html)