



مجلس الأمن السيبراني  
CYBER SECURITY COUNCIL



**Security Updates- Chrome OS**  
Tracking #:432316499  
Date:12-11-2024

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

## TECHNICAL DETAILS:

Google has released a new Long Term Support (LTS) channel update for ChromeOS devices. This update addresses several critical and high-severity security vulnerabilities.

This update includes patches for the following vulnerabilities:

- **Critical** - CVE-2024-10487: Out of bounds write in Dawn
- High - CVE-2024-10231: Type confusion in V8
- High - CVE-2024-10229: Inappropriate implementation in Extensions
- Medium - CVE-2024-9958: Inappropriate implementation in Picture-in-Picture
- Medium - CVE-2024-9963: Insufficient data validation in Downloads

Successful exploitation of these vulnerabilities could potentially allow attackers to execute arbitrary code, escalate privileges, or cause denial of service on affected ChromeOS devices.

### Fixed Version:

- LTS-126 Version: 126.0.6478.257(Platform Version: 15886.82.0)

## RECOMMENDATIONS:

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

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/2024/11/long-term-support-channel-update-for.html>
- <https://chromereleases.googleblog.com/>