



مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Security Updates – ChromeOS

Tracking #:432316360

Date:03-10-2024

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 ChromeOS.

TECHNICAL DETAILS:

Google has released security updates to address multiple vulnerabilities in ChromeOS. These vulnerabilities could potentially allow an attacker to gain unauthorized access to a device or execute malicious code.

This release includes upstream updates to CUPS components and the removal of cups-browsed. When booted in verified mode, ChromeOS devices are not affected by CVE-2024-47076, CVE-2024-47175, CVE-2024-47176, and CVE-2024-47177.

Affected Systems:

- All ChromeOS devices on the ChromeOS Long Term Support (LTS) channel (and not pinned to 120)

Fixed Versions:

- ChromeOS LTS 126.0.6478.254 (Platform Version: 15886.79.0).

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to update ChromeOS to the latest version.

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/2024/10/long-term-support-lts-channel-for.html>
- <https://chromereleases.googleblog.com/>