مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Security Updates – ChromeOS

Tracking #:432316324

Date:24-09-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Google has released security updates to address multiple vulnerabilities for ChromeOS.

TECHNICAL DETAILS:

Google has released a security update for ChromeOS that addresses several vulnerabilities, including multiple high and medium severity issues. This update specifically targets use-after-free vulnerabilities and heap buffer overflow problems, enhancing the overall security posture of the operating system.

Vulnerabilities Details:

- CVE-2024-6989: High severity issue related to a use-after-free vulnerability in Loader.
- CVE-2024-8362: High severity issue concerning a use-after-free vulnerability in WebAudio.
- CVE-2024-7967: High severity heap buffer overflow found in Fonts.
- CVE-2024-8193: High severity heap buffer overflow in Skia.
- CVE-2024-8198: Another high severity heap buffer overflow in Skia.
- CVE-2024-7976: Medium severity issue regarding an inappropriate implementation in FedCM.

Fixed Versions:

- LTC-126 version 126.0.6478.253 (Platform Version: 15886.78.0)

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/2024/09/long-term-support-channel-update-for_23.html