

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Security Updates-ChromeOS

Tracking #:432317745

Date:23-09-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Google has released a new Long-Term Support (LTS) version for ChromeOS that addresses multiple security vulnerabilities.

TECHNICAL DETAILS:

Google has released a new Long-Term Support (LTS) version 132.0.6834.244 (Platform Version: 16093.118.0) for ChromeOS. This release addresses multiple security vulnerabilities, including a critical use-after-free flaw in ServiceWorker (CVE-2025-10200) and a medium-severity issue in File Picker (CVE-2025-8881).

Successful exploitation of these vulnerabilities could allow attackers to execute arbitrary code, escalate privileges, or cause denial of service. Given the presence of a critical memory corruption vulnerability, immediate action is strongly recommended.

Vulnerability Details

1. CVE-2025-8881 – Inappropriate Implementation in File Picker

- **Severity:** Medium
- **Impact:** An attacker could exploit improper implementation in File Picker to bypass security restrictions or access unintended files.
- **Potential Risk:** Data exposure, unauthorized access.

2. CVE-2025-10200 – Use-After-Free in ServiceWorker

- **Severity:** Critical
- **Impact:** A use-after-free vulnerability in ServiceWorker could enable remote code execution (RCE) or privilege escalation if exploited.
- **Potential Risk:** Full device compromise, execution of malicious code, persistence mechanisms.

Fixed Versions:

- LTS version 132.0.6834.244 (Platform Version: 16093.118.0)

RECOMMENDATIONS:

- **Immediate Upgrade:** Ensure all ChromeOS devices are upgraded to fixed 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/2025/09/long-term-support-channel-update-for_19.html?m=1