مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates – Chrome OS
Tracking #:432317986
Date:11-11-2025

TLP: WHITE

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 Long Term Support (LTS) Channel Update for ChromeOS addressing multiple high-severity vulnerabilities that could allow attackers to execute arbitrary code, cause system crashes, or compromise user data.

High-Severity Vulnerabilities:
- **CVE-2025-11756 – Use after free in Safe Browsing**
  A use-after-free vulnerability in the Safe Browsing component could lead to memory corruption and potential arbitrary code execution.
- **CVE-2025-11460 – Use after free in Storage**
  A use-after-free vulnerability in the Storage component could allow attackers to cause a system crash or execute arbitrary code.
- **CVE-2025-12036 – Inappropriate implementation in V8**
  An inappropriate implementation in the V8 JavaScript engine could enable remote code execution when processing malicious web content.
- **CVE-2025-8879 – Heap buffer overflow in libaom**
  A heap buffer overflow in the libaom media library could allow an attacker to execute arbitrary code in the context of the browser.

Fixed Versions:
- A new LTS version 138.0.7204.296 (Platform Version: 16295.81.0)

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/2025/11/long-term-support-channel-update-for.html