مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates- HUAWEI Products

Tracking #:432317155

Date:01-05-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that HUAWEI has released its May 2025 monthly security update for flagship phones and tablets, addressing multiple high and critical severity vulnerabilities in both proprietary HarmonyOS modules and third-party libraries.

TECHNICAL DETAILS:

HUAWEI has released its May 2025 monthly security update for flagship phones and tablets, addressing multiple high and critical severity vulnerabilities in both proprietary HarmonyOS modules and third-party libraries. The update primarily targets HarmonyOS 5.0.0 but also includes patches for previous HarmonyOS and EMUI versions.

HUAWEI Proprietary Vulnerabilities (HarmonyOS 5.0.0)

CVE	Module	Severity	Description
CVE-2025-46584	File System	High	Improper authentication logic could allow unauthorized access to sensitive files.
CVE-2025-46585	Kernel	High	Out-of-bounds array read/write could lead to system crashes or denial of service.
CVE-2025-46586	Contacts	Medium	Inadequate permission controls may disrupt contact management or expose contact data.
CVE-2025-46587	Media Library	Medium	Weak permission controls risk unauthorized access to media files.
CVE-2024-58252	Media Library	Medium	Insufficient information protection may leak sensitive media metadata or content.
CVE-2025-46588	App Lock	Medium	Unauthorized access could bypass app lock protections, exposing or altering app data.
CVE-2025-46589	App Lock	Medium	Similar to above, further weakening app lock security.
CVE-2025-46590	Network Search Auth	Medium	Attackers could bypass authentication to access network search functions.
CVE-2025-46591	Authorization	Medium	Out-of-bounds data read could leak sensitive authorization data.
CVE-2025-46592	USB HDI Driver	Medium	Null pointer dereference may cause device instability when using USB peripherals.
CVE-2025-46593	Print Module	Medium	Process residence in abnormal scenarios

CVE	Module	Severity	Description
			could degrade device performance or availability.

Third-Party Library Vulnerabilities:

- **Critical Severity**:
  - CVE-2025-22423, CVE-2025-26416, CVE-2025-0084
    Affect multiple HarmonyOS (2.0.0–4.3.0) and EMUI (12.0.0–14.0.0) versions. Exploitation could lead to remote code execution or full device compromise.
- **High Severity**:
  - CVE-2024-49730, CVE-2025-22416, CVE-2025-22422, CVE-2025-22427, CVE-2025-22428, CVE-2025-22433, CVE-2025-22438, CVE-2025-22439, CVE-2024-43066, CVE-2024-50264, CVE-2024-53150, CVE-2024-53197, CVE-2025-21429, CVE-2025-21430, CVE-2025-21435, CVE-2025-0082, CVE-2025-0083, CVE-2025-26417, CVE-2025-0079, CVE-2023-21125
    These issues affect a wide range of HarmonyOS and EMUI versions, exposing devices to privilege escalation, information disclosure, and denial of service.
- **Low Severity**:
  - CVE-2025-27248, CVE-2025-25052, CVE-2025-27132, CVE-2025-22886, CVE-2025-27241, CVE-2025-25218
    Affect HarmonyOS 5.0.0, with lower risk but still recommended for patching.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to patch all Huawei devices running HarmonyOS or EMUI using official OTA (over-the-air) updates to address all CVEs listed.

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://consumer.huawei.com/en/support/bulletin/2025/5/