



**Security Updates - Huawei** Tracking #:432317568 Date:05-08-2025

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 INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

The UAE Cyber Security Council has observed that Huawei has released security updates to address multiple vulnerabilities in its flagship models. [COMMENT: Missing execution or effective date | Suggestion: Specify ADGM Courts as governing jurisdiction and ensure required ADGM documents are included. | Citation: ADGM Companies Regulations 2020 (general guidance)]



ADVISORY

EXECUTIVE SUMMARY:

TECHNICAL DETAILS:

HUAWEI has released its August 2025 security bulletin for HarmonyOS and EMUI devices, addressing multiple high- and medium-severity vulnerabilities across various system components and third- party libraries. These vulnerabilities, if exploited, may impact confidentiality, availability, stability, or service integrity of affected devices.

**Vulnerability Details** (including but not limited to):

|  |  |  |  |
| --- | --- | --- | --- |
| **CVE** | **Description** | **Impact** | **Severity** |
| CVE-2025-54607 | Authentication management vulnerability in the ArkWeb module | Successful exploitation of this vulnerability may affect service confidentiality. | High |
| CVE-2025-54611 | EXTRA\_REFERRER resource read vulnerability in the Gallery module | Successful exploitation of this vulnerability may affect service confidentiality. | High |
| CVE-2025-54622 | Binding authentication bypass vulnerability in the devicemanager module | Successful exploitation of this vulnerability may affect service confidentiality. | High |
| CVE-2025-54627 | Out-of-bounds write vulnerability in the skia module | Successful exploitation of this vulnerability may affect service confidentiality. | High |

**Affected/Fixed Versions**: Refer [Security Bulletins for HUAWEI Phones/Tablets, August 2025](https://consumer.huawei.com/en/support/bulletin/2025/8/)

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying latest updates released by the Huawei.

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/2025/8/

https:[//www.csc.gov.ae/](http://www.csc.gov.ae/)

**TLP: WHITE**

Review Comments (Corporate Agent)

**Review Comments (Corporate Agent)**

**1. Section: Clarity**

Issue: Ambiguous or non-binding language

Severity: Medium

Suggestion: Specify ADGM Courts as governing jurisdiction and ensure required ADGM documents are included.

Citation: ADGM Companies Regulations 2020 (general guidance)

**2. Section: Signatures**

Issue: Missing signatory section

Severity: High

Suggestion: Specify ADGM Courts as governing jurisdiction and ensure required ADGM documents are included.

Citation: ADGM Companies Regulations 2020 (general guidance)

**3. Section: Execution**

Issue: Missing execution or effective date

Severity: Low

Suggestion: Specify ADGM Courts as governing jurisdiction and ensure required ADGM documents are included.

Citation: ADGM Companies Regulations 2020 (general guidance)