ROYAUME DU MAROC
ADMINISTRATION
DE LA DEFENSE NATIONALE
Direction Générale de la Sécurité des Systèmes d'Information

المملكة المغربية
إدارة الدفاع الوطني
المديرية العامة لأمن نظم المعلومات

BULLETIN DE SECURITE

Titre	Vulnérabilités critiques dans les produits Samsung
Numéro de Référence	56841209/25
Date de Publication	12 Septembre 2025
Risque	Critique
Impact	Critique

Systèmes affectés

- les smartphones et tablettes Galaxy fonctionnant sous Android 13, 14, 15 et 16.

Identificateurs externes

- CVE-2025-8109 CVE-2025-48581 CVE-2025-48563
- CVE-2025-48562 CVE-2025-48561 CVE-2025-48560
- CVE-2025-48559 CVE-2025-48558 CVE-2025-48557
- CVE-2025-48556 CVE-2025-48554 CVE-2025-48553
- CVE-2025-48552 CVE-2025-48551 CVE-2025-48550
- CVE-2025-48549 CVE-2025-48548 CVE-2025-48547
- CVE-2025-48546 CVE-2025-48545 CVE-2025-48544
- CVE-2025-48543 CVE-2025-48542 CVE-2025-48541
- CVE-2025-48540 CVE-2025-48539 CVE-2025-48538
- CVE-2025-48537 CVE-2025-48535 CVE-2025-48534
- CVE-2025-48532 CVE-2025-48524 CVE-2025-47329
- CVE-2025-47328 CVE-2025-47326 CVE-2025-47318
- CVE-2025-47317 CVE-2025-46710 CVE-2025-46708
- CVE-2025-46707 CVE-2025-38352 CVE-2025-32346
- CVE-2025-32327 CVE-2025-32323 CVE-2025-32322
- CVE-2025-3212 CVE-2025-32100 CVE-2025-27034
- CVE-2025-27032 CVE-2025-26464 CVE-2025-26447

- CVE-2025-25180 CVE-2025-25179 CVE-2025-21756
- CVE-2025-21701 CVE-2025-21488 CVE-2025-21487
- CVE-2025-21484 CVE-2025-21483 CVE-2025-21482
- CVE-2025-21481 CVE-2025-21043 CVE-2025-21034
- CVE-2025-21033 CVE-2025-21032 CVE-2025-21031
- CVE-2025-21030 CVE-2025-21029 CVE-2025-21028
- CVE-2025-21027 CVE-2025-21026 CVE-2025-21025
- CVE-2025-20708 CVE-2025-20704 CVE-2025-20703
- CVE-2025-1706 CVE-2025-1246 CVE-2025-0467
- CVE-2025-0089 CVE-2024-7881 CVE-2024-47899
- CVE-2024-47898 CVE-2023-40130

Bilan de la vulnérabilité

Samsung a publié son « Security Maintenance Release (SMR) » de septembre 2025, corrigeant plusieurs vulnérabilités critiques affectant les produits susmentionnés. Parmi ces vulnérabilités, une faille critique « CVE-2025-21043 » de type zero-day, dans la bibliothèque "libimagecodec.quram.so" est activement exploitée. Cette faille permet à un attaquant distant d'exécuter du code arbitraire sur un appareil vulnérable en incitant l'utilisateur à traiter une image spécialement conçue.

En complément, plusieurs vulnérabilités de haute et moyenne gravité ont été corrigées, permettant notamment de bloquer diverses attaques, notamment l'exécution de code local par des applications malveillantes, la divulgation d'informations sensibles, la perturbation des communications (interruption d'appels, désactivation de la SIM), ainsi que le contournement des mesures de sécurité tels que le « Kiosk Mode » et la gestion des privilèges.

Solution :

Veuillez se référer au bulletin de sécurité Samsung du 12 Septembre2025 pour plus d'infirmation.

Risque :

- Exécution de code arbitraire à distance (RCE)
- Exécution de code local

- Atteinte à la confidentialité des données
- Atteinte à l’intégrité des données
- Divulgation d’informations sensibles
- Perturbation des communications
- Contournement des mesures de sécurité

Annexe

Bulletin de sécurité Samsung du 12 Septembre2025**:**

- https://security.samsungmobile.com/securityUpdate.smsb

Direction Générale de la Sécurité des Systèmes d’Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques, Méchouar Saïd,
B.P. 1048 Rabat – Tél : 05 37 57 21 47 – Fax : 05 37 57 20 53
Email : contact@macert.gov.ma

المديرية العامة لأمن نظم المعلومات ,مديرية تدبير مركز اليقظة والرصد والتصدي للهجمات المعلوماتية ، المشور السعيد، ص.ب. 1048 الرباط
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma