ROYAUME DU MAROC
ADMINISTRATION
DE LA DEFENSE NATIONALE
Direction Générale de la Sécurité des Systèmes d'Information
Centre de Veille de Détection et de Réaction aux Attaques Informatiques

المملكة المغربية
إدارة الدفاع الوطني
المديرية العامة لأمن نظم المعلومات
مركز اليقظة والرصد والتصدي للهجمات المعلوماتية

BULLETIN DE SECURITE

Titre	Vulnérabilités affectant le système d'exploitation Android
Numéro de Référence	43610709/23
Date de publication	07 Septembre 2023
Risque	Important
Impact	Critique

Systèmes affectés

- Google Android versions 11, 12, 12L, 13 sans le correctif de sécurité du 5 Septembre 2023

Identificateurs externes

CVE-2022-40534 CVE-2023-21646 CVE-2023-21653 CVE-2023-28538 CVE-2023-28549
CVE-2023-28573 CVE-2023-28581 CVE-2023-28584 CVE-2023-33015 CVE-2023-33016
CVE-2023-33019 CVE-2023-33021 CVE-2023-35658 CVE-2023-35664 CVE-2023-35665
CVE-2023-35666 CVE-2023-35667 CVE-2023-35669 CVE-2023-35670 CVE-2023-35671
CVE-2023-35673 CVE-2023-35674 CVE-2023-35675 CVE-2023-35676 CVE-2023-35677
CVE-2023-35679 CVE-2023-35680 CVE-2023-35681 CVE-2023-35682 CVE-2023-35683
CVE-2023-35684 CVE-2023-35687

Bilan de la vulnérabilité

Google annonce la correction de plusieurs vulnérabilités affectant son système d'exploitation Android. Une de ces vulnérabilités, identifiée par «CVE-2023-35674» est un Zero-day susceptible d'être activement exploité. L'exploitation de ces vulnérabilités peut permettre à un attaquant distant d'exécuter du code arbitraire, d'accéder à des données confidentielles, d'élever ses privilèges ou de causer un déni de service.

Solution

Veuillez se référer aux bulletins de sécurité d'Android pour mettre à jours vos équipements.

Risque

- Elévation de privilèges
- Exécution de code arbitraire
- Accès à des données confidentielles
- Déni de service

Références

Bulletin de sécurité d'Android :

- https://source.android.com/docs/security/bulletin/2023-09-01?hl=fr