



.....
Centre de Veille de Détection et de
Réaction aux Attaques Informatiques

BULLETIN DE SECURITE

Titre	Vulnérabilités affectant le système d'exploitation Android
Numéro de Référence	41630305/23
Date de publication	03 Mai 2023
Risque	Important
Impact	Critique

Systèmes affectés

- Google Android versions 11, 12, 12L, 13 sans le correctif de sécurité du 1 Mai 2023

Identificateurs externes

CVE-2021-0877	CVE-2021-39617	CVE-2022-20338	CVE-2022-20444	CVE-2022-25713
CVE-2022-33273	CVE-2022-33305	CVE-2022-34144	CVE-2022-40504	CVE-2022-40508
CVE-2022-46394	CVE-2022-46395	CVE-2022-46396	CVE-2022-46891	CVE-2022-47469
CVE-2022-47470	CVE-2022-47486	CVE-2022-47487	CVE-2022-47488	CVE-2023-0266
CVE-2023-20694	CVE-2023-20695	CVE-2023-20696	CVE-2023-20697	CVE-2023-20698
CVE-2023-20699	CVE-2023-20726	CVE-2023-20914	CVE-2023-20930	CVE-2023-20993
CVE-2023-21102	CVE-2023-21103	CVE-2023-21104	CVE-2023-21106	CVE-2023-21107
CVE-2023-21109	CVE-2023-21110	CVE-2023-21111	CVE-2023-21112	CVE-2023-21116
CVE-2023-21117	CVE-2023-21118	CVE-2023-21665	CVE-2023-21666	CVE-2023-26085

Bilan de la vulnérabilité

Google annonce la correction de plusieurs vulnérabilités affectant son système d'exploitation Android. 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

Veillez 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
- Dénier de service

Références

Bulletin de sécurité d'Android :

- <https://source.android.com/docs/security/bulletin/2023-05-01?hl=fr>