



BULLETIN DE SECURITE

Titre	Vulnérabilités affectant le système d'exploitation Android
Numéro de Référence	40700803/23
Date de publication	08 Février 2023
Risque	Important
Impact	Critique

Systemes affectés

- Google Android versions 11, 12, 12L, 13 sans le correctif de sécurité du 6 Mars 2023

Identificateurs externes

CVE-2021-33655	CVE-2023-20906	CVE-2023-20911	CVE-2023-20917
CVE-2023-20947	CVE-2023-20963	CVE-2023-20956	CVE-2023-20958
CVE-2023-20964	CVE-2023-20951	CVE-2023-20954	CVE-2023-20926
CVE-2023-20931	CVE-2023-20936	CVE-2023-20953	CVE-2023-20955
CVE-2023-20957	CVE-2023-20959	CVE-2023-20960	CVE-2023-20966
CVE-2022-4452	CVE-2022-20467	CVE-2023-20929	CVE-2023-20952
CVE-2023-20962	CVE-2022-20499	CVE-2023-20910	CVE-2022-47459
CVE-2022-47461	CVE-2022-47462	CVE-2022-47460	CVE-2022-22075
CVE-2022-40537	CVE-2022-40540	CVE-2022-33213	CVE-2022-33256
CVE-2022-25655	CVE-2022-25694	CVE-2022-25705	CVE-2022-25709
CVE-2022-33242	CVE-2022-33244	CVE-2022-33250	CVE-2022-33254
CVE-2022-33272	CVE-2022-33278	CVE-2022-33309	CVE-2022-40515
CVE-2022-40527	CVE-2022-40530	CVE-2022-40531	CVE-2022-40535
CVE-2023-20620	CVE-2023-20621	CVE-2023-20623	

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
- Déni de service

Références

Bulletin de sécurité d'Android :

- <https://source.android.com/docs/security/bulletin/2023-03-01>