



.....
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	43200908/23
Date de publication	09 aout 2023
Risque	Important
Impact	Critique

Systèmes affectés

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

Identificateurs externes

CVE-2020-29374	CVE-2022-34830	CVE-2022-40510	CVE-2023-20780	CVE-2023-20965
CVE-2023-21132	CVE-2023-21133	CVE-2023-21134	CVE-2023-21140	CVE-2023-21242
CVE-2023-21264	CVE-2023-21265	CVE-2023-21267	CVE-2023-21268	CVE-2023-21269
CVE-2023-21270	CVE-2023-21271	CVE-2023-21272	CVE-2023-21273	CVE-2023-21274
CVE-2023-21275	CVE-2023-21276	CVE-2023-21277	CVE-2023-21278	CVE-2023-21279
CVE-2023-21280	CVE-2023-21281	CVE-2023-21282	CVE-2023-21283	CVE-2023-21284
CVE-2023-21285	CVE-2023-21286	CVE-2023-21287	CVE-2023-21288	CVE-2023-21289
CVE-2023-21290	CVE-2023-21292	CVE-2023-21626	CVE-2023-21627	CVE-2023-21647
CVE-2023-21648	CVE-2023-21649	CVE-2023-21650	CVE-2023-22666	CVE-2023-28537
CVE-2023-28555				

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/2023-08-01>