



BULLETIN DE SECURITE

Titre	Vulnérabilités affectant le système d'exploitation Android
Numéro de Référence	45060612/23
Date de publication	06 Décembre 2023
Risque	Important
Impact	Critique

Systemes affectés

- Google Android versions 11, 12, 12L, 13 et 14 sans le correctif de sécurité du 4 Décembre 2023

Identificateurs externes

CVE-2022-22076	CVE-2022-40507	CVE-2022-48454	CVE-2022-48455	CVE-2022-48456
CVE-2022-48457	CVE-2022-48458	CVE-2022-48459	CVE-2022-48461	CVE-2023-21162
CVE-2023-21163	CVE-2023-21164	CVE-2023-21166	CVE-2023-21215	CVE-2023-21216
CVE-2023-21217	CVE-2023-21218	CVE-2023-21227	CVE-2023-21228	CVE-2023-21263
CVE-2023-21267	CVE-2023-21394	CVE-2023-21401	CVE-2023-21402	CVE-2023-21403
CVE-2023-21652	CVE-2023-21662	CVE-2023-21664	CVE-2023-28546	CVE-2023-28550
CVE-2023-28551	CVE-2023-28585	CVE-2023-28586	CVE-2023-28587	CVE-2023-28588
CVE-2023-32804	CVE-2023-32818	CVE-2023-32847	CVE-2023-32848	CVE-2023-32850
CVE-2023-32851	CVE-2023-33017	CVE-2023-33018	CVE-2023-33022	CVE-2023-33053
CVE-2023-33054	CVE-2023-33063	CVE-2023-33079	CVE-2023-33080	CVE-2023-33081
CVE-2023-33087	CVE-2023-33088	CVE-2023-33089	CVE-2023-33092	CVE-2023-33097
CVE-2023-33098	CVE-2023-33106	CVE-2023-33107	CVE-2023-35668	CVE-2023-35690
CVE-2023-3889	CVE-2023-40073	CVE-2023-40074	CVE-2023-40075	CVE-2023-40076
CVE-2023-40077	CVE-2023-40078	CVE-2023-40079	CVE-2023-40080	CVE-2023-40081
CVE-2023-40082	CVE-2023-40083	CVE-2023-40084	CVE-2023-40087	CVE-2023-40088
CVE-2023-40089	CVE-2023-40090	CVE-2023-40091	CVE-2023-40092	CVE-2023-40094
CVE-2023-40095	CVE-2023-40096	CVE-2023-40097	CVE-2023-40098	CVE-2023-40103
CVE-2023-4272	CVE-2023-45773	CVE-2023-45774	CVE-2023-45775	CVE-2023-45776
CVE-2023-45777	CVE-2023-45779	CVE-2023-45781	CVE-2023-45866	

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/2023-12-01?hl=fr>