



BULLETIN DE SECURITE

Titre	Vulnérabilités affectant le système d'exploitation Android
Numéro de Référence	46360703/24
Date de publication	07 Septembre 2023
Risque	Important
Impact	Critique

Systemes affectés

- Google Android versions 12, 12L, 13 et 14 sans le correctif de sécurité de Mars 2024

Identificateurs externes

CVE-2023-28578	CVE-2023-33042	CVE-2023-33066	CVE-2023-33105	CVE-2023-40081
CVE-2023-43539	CVE-2023-43546	CVE-2023-43547	CVE-2023-43548	CVE-2023-43549
CVE-2023-43550	CVE-2023-43552	CVE-2023-43553	CVE-2023-48424	CVE-2023-48425
CVE-2023-6143	CVE-2023-6241	CVE-2024-0039	CVE-2024-0044	CVE-2024-0045
CVE-2024-0046	CVE-2024-0047	CVE-2024-0048	CVE-2024-0049	CVE-2024-0050
CVE-2024-0051	CVE-2024-0052	CVE-2024-0053	CVE-2024-20005	CVE-2024-20020
CVE-2024-20022	CVE-2024-20023	CVE-2024-20024	CVE-2024-20025	CVE-2024-20026
CVE-2024-20027	CVE-2024-20028	CVE-2024-23717		

Bilan de la vulnérabilité

Google annonce la correction de plusieurs vulnérabilités affectant son système d'exploitation Android. Deux de ces vulnérabilités, identifiées par «CVE-2024-0039» et « CVE-2024-23717 » sont critiques. 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/2024-03-01?hl=fr>