



BULLETIN DE SECURITE

Titre	Vulnérabilités critiques dans Android et Pixel
Numéro de Référence	41620205 /23
Date de Publication	02 Mai 2023
Risque	Critique
Impact	Critique

Systèmes affectés

- Google Android et Pixel toutes versions sans le correctif de sécurité du 01 mai 2023

Identificateurs externes

- CVE-2021-39617 , CVE-2022-20338 , CVE-2023-20993 , CVE-2023-21109 , CVE-2023-21117 , CVE-2023-20914 , CVE-2023-21104 , CVE-2023-20930 , CVE-2023-21116 , CVE-2023-21110 , CVE-2022-20444 , CVE-2023-21107 , CVE-2023-21112 , CVE-2023-21118 , CVE-2023-21103 , CVE-2023-21111 , CVE-2023-21102 , CVE-2023-21106 , CVE-2023-0266 , CVE-2022-4639 , CVE-2022-46395 , CVE-2022-46396 , CVE-2022-46891 , CVE-2023-26085 , CVE-2021-0877 , CVE-2023-20694 , CVE-2023-20695 , CVE-2023-20696 , CVE-2023-20699 , CVE-2023-20697 , CVE-2023-20698 , CVE-2023-20726 , CVE-2022-47469 , CVE-2022-47470 , CVE-2022-47486 , CVE-2022-47487 , CVE-2022-47488 , CVE-2023-21665 , CVE-2023-21666 , CVE-2022-25713 , CVE-2022-33273 , CVE-2022-33305 , CVE-2022-34144 , CVE-2022-40504 , CVE-2022-40508 , CVE-2023-21119 , CVE-2022-33281

Bilan de la vulnérabilité

Plusieurs vulnérabilités critiques ont été corrigées dans le système d'exploitation Android et pixel. L'exploitation de ces vulnérabilités peut permettre à un attaquant de réussir une élévation de privilèges, de causer un déni de service, d'exécuter du code arbitraire ou de porter atteinte à la confidentialité des données.

Solution :

Veillez se référer au bulletin de sécurité Android du 01 mai 2023 pour plus d'informations.

Risque :

- Exécution de code arbitraire à distance
- Dénier de service à distance
- Atteinte à la confidentialité des données
- Élévation de privilèges

Annexe

Bulletin de sécurité Android du 01 mai 2023 :

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