

A background visualization of a network or data flow, featuring glowing blue nodes and connecting lines, with some nodes labeled with numbers like 2789, 3659, 4617, and 5013.

Bulletin d'alerte Vulnérabilité critique dans Google Nest

Sommaire

GOOGLE	2
Google Nest - CVE-2023-48419	2
Type de vulnérabilité.....	2
Risques.....	2
Criticité (score de base CVSS v3.1).....	2
Produits impactés.....	2
Recommandations.....	3
Preuve de concept.....	3
RÉFÉRENCES	4

GOOGLE

Google a publié un bulletin de sécurité le 11 décembre 2023 concernant une vulnérabilité **critique** dans **Nest**, son outil de synchronisation domotique pour des réseaux domestiques.

Google Nest - CVE-2023-48419



Les chercheurs en sécurité ont découvert une faille affectant les appareils connectés de **Google Nest**. Des mises à jour OTA (*Over-the-Air*) automatiques ont été déployées au cours du mois de décembre 2023.

Peu de détails techniques sont révélés. L'exploitation de cette vulnérabilité par un attaquant se trouvant à proximité d'un réseau Wi-Fi d'un Google Home peut espionner la victime et élever ses privilèges..

Type de vulnérabilité

- **CWE-269**: Improper Privilege Management

Risques

- Élévation des privilèges

Criticité (score de base CVSS v3.1)

Vecteur d'attaque	Réseau	Portée	Changée
Complexité d'attaque	Faible	Impact sur la confidentialité	Élevé
Privilèges requis	Aucun	Impact sur l'intégrité	Élevé
Interaction de l'utilisateur	Aucune	Impact sur la disponibilité	Élevé

Produits impactés

Micrologiciel de gestion des systèmes ou appareils suivants :

- Google Nest Audio
- Google Nest Mini
- Google Home Mini
- Google Home

Recommandations

Google a déployé des mises à jour automatiques vers la version 2.58 de son micrologiciel des appareils vulnérables au cours du mois de décembre 2023. Aucune action n'est requise de la part des utilisateurs.

Site de l'éditeur

- Des informations complémentaires sont disponibles sur le [bulletin Google](#).

Preuve de concept

Aucune preuve de concept n'est disponible en source ouverte.

Références

GOOGLE

- https://support.google.com/product-documentation/answer/14273332?hl=en&ref_topic=12974021&sjid=4533873659772963473-NA#zippy=%2Cspeakers

CVE-2023-48419

- <https://nvd.nist.gov/vuln/detail/CVE-2023-48419>
- <https://vuldb.com/fr/?id.249528>