

The background of the page is a complex network visualization with glowing blue nodes and connecting lines, set against a dark background. Some nodes are labeled with numbers like 5013, 2789, 3659, and 4617.

Bulletin d'alerte Vulnérabilité critique dans Google Chrome

Sommaire

GOOGLE	2
Chrome - CVE-2023-7024	2
Type de vulnérabilité.....	2
Risques.....	2
Criticité (score de base CVSS v3.1).....	2
Produit impacté.....	2
Recommandations.....	2
Preuve de concept.....	3
RÉFÉRENCES	4

Google

Le 20/12/2023, [Google](#) a publié une mise à jour d'urgence pour corriger une faille *zéro-day* **exploitée** dans le navigateur Web Chrome.

Chrome - CVE-2023-7024



Les chercheurs en sécurité Clément Lecigne et Vlad Stolyarov du Google Threat Analysis Group (TAG) ont identifié une faille de dépassement de la mémoire tampon dans le composant *WebRTC* de Google Chrome.

L'exploitation de cette faille par un attaquant distant et non authentifié permet, en persuadant une victime de consulter un site Web spécifiquement forgé, d'exécuter du code arbitraire et de provoquer un déni de service.



L'éditeur mentionne que la vulnérabilité est activement exploitée.

Type de vulnérabilité

- [CWE-122](#): Heap-based Buffer Overflow

Risques

- Exécution de code arbitraire
- Déni de service

Criticité (score de base CVSS v3.1)

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

Produit impacté

- Google Chrome versions antérieures à 120.0.6099.129 et 120.0.6099.130

Recommandations

Il est recommandé de mettre Google Chrome à jour :

- Vers la version 120.0.6099.129 pour MacOS et Linux,
- Vers la version 120.0.6099.129/130 pour Windows.

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://chromereleases.googleblog.com/2023/12/stable-channel-update-for-desktop_20.html

CVE-2023-7024

- <https://securityaffairs.com/156231/security/google-addressed-a-new-actively-exploited-chrome-zero-day.html>
- <https://exchange.xforce.ibmcloud.com/vulnerabilities/275490>
- <https://vuldb.com/?id.248580>