aDvens

Security for the greater good

Bulletin d’alerte

Vulnérabilité critique dans Google Chrome

2024-01-17 | **TLP:CLEAR** | CERT aDvens - CTI

Advens - 16 Quai de la Mégisserie - 75001 Paris

aDvens

Sommaire

Google Chrome - CVE-2024-0519

Le 16 janvier 2024, Google a publié un correctif corrigeant 3 vulnérabilités dans Chrome dont une zéro-day exploitée. Cette dernière est due à un défaut de contrôle de la mémoire (*out-of-bounds memory access*) dans le moteur V8.

En persuadant une victime de consulter un site web spécifiquement forgé, un attaquant peut exécuter du code arbitraire et provoquer un déni de service.

Cette vulnérabilité est activement exploitée.

Type de vulnérabilité

- **CWE-125** : Out-of-bounds Read

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 120.0.6099.224 sur Windows et Linux
- versions antérieures à 120.0.6099.234 sur macOS

Recommandations

- Mettre à jour Google Chrome vers la version 120.0.6099.224 sur Linux, 120.0.6099.224/225 sur Windows et 120.0.6099.234 sur macOS.
- Des informations complémentaires sont disponibles dans le bulletin de Google.

Preuve de concept

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

Références

- https://www.cve.org/CVERecord?id=CVE-2024-0519
- https://chromereleases.googleblog.com/2024/01/stable-channel-update-for-desktop_16.html
- https://www.bleepingcomputer.com/news/security/google-fixes-first-actively-exploited-chrome-zero-day-of-2024/