



BULLETIN DE SECURITE

Titre	Vulnérabilité critique dans la bibliothèque lipwebp
Numéro de Référence	43992709/23
Date de Publication	27 Septembre 2023
Risque	Critique
Impact	Critique

Systemes affectés

- lipwebp versions entre 0.5.0 et 1.3.2

Identificateurs externes

- CVE-2023-5129

Bilan de la vulnérabilité

Des chercheurs en sécurité ont découvert une vulnérabilité critique de type zero-day (CVE-2023-5129) affectant la bibliothèque open-source « lipwebp », une bibliothèque de compression d'images utilisée dans Chromium et d'autres solutions logicielles prenant en charge les images « WebP ». La vulnérabilité a un score CVSSv3 (Common Vulnerability Scoring System) de 10 sur 10 et activement exploitée.

L'exploitation de la vulnérabilité de débordement de mémoire pourrait permettre à un attaquant de causer un déni de service, exécuter du code arbitraire et porter atteinte à la confidentialité des données.

Solution

Veillez se référer au bulletin de sécurité lipwebp afin d'installer les nouvelles mises à jour.

Risque

- Exécution de code arbitraire
- Déni de service
- Atteinte à la confidentialité des données

Annexe

Bulletin de sécurité lipwebp:

- <https://nvd.nist.gov/vuln/detail/CVE-2023-5129>
- <https://chromium.googlesource.com/webm/libwebp/+902bc9190331343b2017211debcc8d2ab87e17a>