



BULLETIN DE SECURITE

Titre	Vulnérabilités critiques dans Google Chrome
Numéro de Référence	63231604/26
Date de Publication	16 Avril 2026
Risque	Critique
Impact	Critique

Systèmes affectés

- Chrome versions antérieures à 147.0.7727.101 pour Linux ;
- Chrome versions antérieures à 147.0.7727.101/102 pour Windows ;
- Chrome versions antérieures à 147.0.7727.101/102 pour Mac ;

Identificateurs externes

- CVE-2026-6296 CVE-2026-6297 CVE-2026-6298 CVE-2026-6299 CVE-2026-6300
- CVE-2026-6301 CVE-2026-6302 CVE-2026-6303 CVE-2026-6304 CVE-2026-6305
- CVE-2026-6306 CVE-2026-6307 CVE-2026-6308 CVE-2026-6309 CVE-2026-6310
- CVE-2026-6311 CVE-2026-6312 CVE-2026-6313 CVE-2026-6314 CVE-2026-6315
- CVE-2026-6316 CVE-2026-6317 CVE-2026-6318 CVE-2026-6319 CVE-2026-6358
- CVE-2026-6359 CVE-2026-6360 CVE-2026-6361 CVE-2026-6362 CVE-2026-6363
- CVE-2026-6364

Bilan de la vulnérabilité

Google a publié des mises à jour de sécurité pour corriger plusieurs vulnérabilités critiques affectant Google chrome. L'exploitation de ces failles peut permettre à un attaquant de causer un déni de service, de porter atteinte à la confidentialité des données, d'exécuter du code arbitraire à distance et de prendre le contrôle du système affecté.

Solution

Veillez se référer au bulletin de sécurité Google du 15 Avril 2026 pour plus d'information.

Risque

- Prise de contrôle du système affecté ;
- Exécution du code arbitraire à distance ;

- Déni de service ;
- Atteinte à la confidentialité des données ;

Annexe

Bulletin de sécurité Google 15 Avril 2026:

- https://chromereleases.googleblog.com/2026/04/stable-channel-update-for-desktop_15.html