



BULLETIN DE SECURITE

| | |
|----------------------------|--|
| Titre | Zero-days activement exploités affectant le navigateur Google Chrome |
| Numéro de Référence | 62031303/26 |
| Date de Publication | 16 Mars 2026 |
| Risque | Important |
| Impact | Critique |

Systemes affectés

- Google Chrome versions antérieures à 146.0.76380.119 (Android)
- Google Chrome versions antérieures à 146.0.7680.80 (Linux)
- Google Chrome versions antérieures à 146.0.7680.80 (Mac)
- Google Chrome versions antérieures à 146.0.7680.80 (Windows)

Identificateurs externes

- CVE-2026-3909 CVE-2026-3910

Bilan de la vulnérabilité

Google vient de publier une mise à jour de sécurité qui permet de corriger deux « Zero-days » affectant le navigateur Google Chrome. Ces vulnérabilités sont activement exploitées et peuvent permettre à un attaquant d'exécuter du code à distance ou de contourner des mesures de sécurité.

Solution

Veillez se référer aux bulletins de Google afin d'installer les nouvelles mises à jour.

Risques

- Exécution de code à distance
- Contournement de mesures de sécurité

Références

Bulletins de sécurité Google:

- https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_12.html
- https://chromereleases.googleblog.com/2026/03/chrome-for-android-update_12.html
- https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_13.html
- https://chromereleases.googleblog.com/2026/03/chrome-for-android-update_13.html