AVIS DE SECURITE

Objet	Multiples vulnérabilités critiques dans Google Chrome (version 153)
Niveau de criticité	**CRITIQUE**
Référence	SNCSIRT-2026-ADS-199
TLP	WHITE

Résumé

Google a promu Chrome 153 (153.0.8010.36/.37) au canal stable le 8 septembre 2026, corrigeant 230 failles de sécurité dont 5 classées « Critical » par Chromium, principalement des use-after-free et débordements de mémoire dans le moteur WebGL et dans le composant Cast, pouvant permettre à un attaquant distant d'exécuter du code arbitraire hors du bac à sable via une page HTML ou un flux réseau spécialement conçus. Google indique par ailleurs qu'un exploit existe dans la nature pour une vulnérabilité distincte de sévérité Medium (CVE-2026-87491, V8) corrigée dans la même mise à jour.

Risque de sécurité

- Exécution de code arbitraire à distance hors du bac à sable (CVE-2026-87464, Use after free dans WebGL, Critical)
- Exécution de code arbitraire à distance hors du bac à sable (CVE-2026-87488, Use after free dans WebGL, Critical)
- Exécution de code arbitraire à distance hors du bac à sable (CVE-2026-87438, Out of bounds write dans WebGL, Critical)
- Exécution de code arbitraire à distance hors du bac à sable (CVE-2026-87527, Buffer overflow dans WebGL, Critical)
- Exécution de code arbitraire à distance hors du bac à sable (CVE-2026-87628, Use after free dans Cast, Critical)

Systèmes affectés

- Google Chrome pour Windows et Mac : versions antérieures à 153.0.8010.36/.37
- Google Chrome pour Linux : versions antérieures à 153.0.8010.36

Recommandations

1. Se référer au bulletin de sécurité de l'éditeur du 08 septembre 2026 :

- https://chromereleases.googleblog.com/2026/09/stable-channel-update-for-desktop_0808145027.html