



## BULLETIN DE SECURITE

|                            |                             |
|----------------------------|-----------------------------|
| <b>Titre</b>               | Zero-day dans Google Chrome |
| <b>Numéro de Référence</b> | 58591911/25                 |
| <b>Date de Publication</b> | 19 Novembre 2025            |
| <b>Risque</b>              | Critique                    |
| <b>Impact</b>              | Critique                    |

### Systèmes affectés

- Google Chrome versions antérieures à 142.0.7444.175 pour Linux
- Google Chrome versions antérieures à 142.0.7444.175/.176 pour Windows et Mac

### Identificateurs externes

- CVE-2025-13223, CVE-2025-13224

### Bilan de la vulnérabilité

Google a publié une mise à jour de sécurité urgente pour le navigateur Chrome, corrigeant deux vulnérabilités critiques, dont une faille zero-day (CVE-2025-13223) déjà exploitée dans des attaques ciblées. Cette vulnérabilité, située dans le moteur V8 JavaScript, permet à un attaquant d'exécuter du code malveillant à distance simplement en incitant l'utilisateur à visiter une page web spécialement conçue.

### Solution

Veuillez se référer au bulletin de sécurité Google du 17 Novembre 2025 pour plus d'information.

### Risque

- Exécution du code arbitraire à distance

### Annexe

Bulletins de sécurité Google du 17 Novembre 2025:

- [https://chromereleases.googleblog.com/2025/11/stable-channel-update-for-desktop\\_17.html](https://chromereleases.googleblog.com/2025/11/stable-channel-update-for-desktop_17.html)