



.....
Centre de Veille de Détection et de
Réaction aux Attaques Informatiques

BULLETIN DE SECURITE

| | |
|----------------------------|---|
| Titre | Zero-Day critique activement exploitée affectant Gogs |
| Numéro de Référence | 59251112/25 |
| Date de publication | 11 Décembre 2025 |
| Risque | Critique |
| Impact | Critique |

Systèmes affectés

- Gogs, toutes les versions

Identificateurs externes

- CVE-2025-8110

Bilan de la vulnérabilité

Une vulnérabilité critique affectant la solution de gestion de dépôts Git auto-hébergée « Gogs » est activement exploitée. Cette vulnérabilité peut permettre à un attaquant distant d'exécuter des commandes.

Solution

Aucune mise à jour n'est disponible pour le moment. Il est recommandé de ne pas exposer votre serveur Gogs à internet en attendant la disponibilité de la mise à jour.

Risque

- Exécution de commandes à distance

Référence

Site web de Gogs :

- <https://gogs.io/>

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques
Informatiques
Tél : 05 37 57 21 47 – Fax : 05 37 57 20 53
Email : contact@macert.gov.ma

المديرية العامة لأمن نظم المعلومات، مديرية تدبير مركز اليقظة والرصد
والتصدي للهجمات المعلوماتية
هاتف: 05 37 57 21 47 – فاكس: 05 37 57 20 53
البريد الإلكتروني contact@macert.gov.ma