



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

BULLETIN DE SECURITE

Titre	Vulnérabilités affectant GLPI
Numéro de Référence	60760502/26
Date de publication	05 février 2026
Risque	Important
Impact	Important

Systèmes affectés

- GLPI versions 11.0.x antérieures à la version 11.0.5
- GLPI versions antérieures à 10.0.23 qui viennent après la version 0.71

Identificateurs externes

- CVE-2026-22044 CVE-2026-22247 CVE-2026-23624

Bilan de la vulnérabilité

Trois vulnérabilités affectant les versions susmentionnées de GLPI ont été corrigées. Un attaquant peut exploiter ces vulnérabilités pour injecter du code SQL, accéder à des données confidentielles ou falsifier des requêtes côté serveur.

Solution

Veuillez se référer aux bulletins de sécurité de l'éditeur pour installer les mises à jour.

Risques

- Injection de code SQL
- Accès à des données confidentielles
- Falsification de requêtes côté serveur (SSRF)

Références

Bulletins de sécurité de GLPI:

- <https://github.com/glpi-project/glpi/security/advisories/GHSA-569q-j526-w385>
- <https://github.com/glpi-project/glpi/security/advisories/GHSA-5j4j-vx46-r477>
- <https://github.com/glpi-project/glpi/security/advisories/GHSA-f6f6-v3qr-9p5x>