ROYAUME DU MAROC
ADMINISTRATION
DE LA DEFENSE NATIONALE
Direction Générale de la Sécurité des Systèmes d'Information
Centre de Veille de Détection et de Réaction aux Attaques Informatiques

المملكة المغربية
إدارة الدفاع الوطني
المديرية العامة لأمن نظم المعلومات
مركز اليقظة والرصد والتصدي للهجمات المعلوماتية

BULLETIN DE SECURITE

Titre	Vulnérabilités affectant le framework AI LangChain
Numéro de Référence	48512507/24
Date de Publication	25 Juillet 2024
Risque	Important
Impact	Important

Systèmes affectés

- LangChain versions antérieures à 0.0.317
- LangChain Experimental versions antérieures à 0.0.306

Identificateurs externes

- CVE-2023-46229 CVE-2023-44467

Bilan de la vulnérabilité

Deux vulnérabilités affectant le framework AI LangChain ont été corrigées. L'exploitation de ces vulnérabilités peut permettre à un attaquant la falsification de requêtes coté serveur ou le contournement de mesures de sécurité.

Solution

Veuillez se référer à l'éditeur afin d'installer les nouvelles mises à jour.

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: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma

Risques

- Contournement de mesures de sécurité
- Falsification de requêtes coté serveur

Références

Article de Palo Alto Networks :

- https://unit42.paloaltonetworks.com/langchain-vulnerabilities/