



BULLETIN DE SECURITE

Titre	Vulnérabilités critiques affectant l'outil d'intelligence artificielle TorchServe
Numéro de Référence	44080410/23
Date de publication	04 Octobre 2023
Risque	Critique
Impact	Critique

Systemes affectés

- TorchServe, versions antérieures à 0.8.2

Identificateurs externes

- CVE-2023-43654 CVE-2022-1471

Bilan de la vulnérabilité

Deux vulnérabilités critiques ont été corrigées au niveau des versions susmentionnées de l'outil d'intelligence artificielle TorchServe. L'exploitation de ces vulnérabilités peut permettre à un attaquant distant d'exécuter du code arbitraire ou d'accéder à des données confidentielles.

Solution

Veillez se référer au bulletin de l'éditeur afin d'installer les nouvelles mises à jour.

Risques

- Exécution de code arbitraire
- Accès à des données confidentielles

Références

Page de TorchServe sur Github :

- <https://github.com/pytorch/serve/blob/master/README.md>