



## BULLETIN DE SECURITE

<b>Titre</b>	Vulnérabilité dans OpenSSL
<b>Numéro de Référence</b>	47683105/24
<b>Date de Publication</b>	31 Mai 2024
<b>Risque</b>	Important
<b>Impact</b>	Important

### Systemes affectés

- OpenSSL versions 1.1.1 antérieures à 1.1.1y
- OpenSSL versions 3.0.x antérieures à 3.0.14
- OpenSSL versions 3.1.x antérieures à 3.1.6
- OpenSSL versions 3.2.x antérieures à 3.2.2
- OpenSSL versions 3.3.x antérieures à 3.3.1

### Identificateurs externes

- CVE-2024-4741

### Bilan de la vulnérabilité

OpenSSL a publié un avis de sécurité pour corriger une vulnérabilité affectant les versions susmentionnées d'OpenSSL. L'exploitation de cette faille peut permettre à un attaquant de causer un déni de service, d'exécuter du code arbitraire à distance et de porter atteinte à la confidentialité des données.

### Solution

Veillez se référer au bulletin de sécurité OpenSSL du 28 Mai 2024 pour plus d'information.

### Risque

- Déni de service à distance
- Exécution du code arbitraire à distance
- Atteinte à la confidentialité de données

### Annexe

Bulletin de sécurité OpenSSL du 28 Mai 2024:

- <https://www.openssl.org/news/secadv/20240528.txt>