AVIS DE SECURITE

Objet	Vulnérabilité dans OpenSSL
Niveau de criticité	**IMPORTANT**
Référence	SNCSIRT-2025-ADS-053
TLP	WHITE

Résumé

OpenSSL a publié un avis de sécurité pour corriger une vulnérabilité (CVE-2024-12797) affectant certaines de ses versions. L'exploitation de cette faille peut permettre à un attaquant de réussir une attaque de type Man-in-the-Middle (MitM).

Risque de sécurité

Réussir une attaque Man-in-the-Middle (MitM)

Systèmes affectés

- OpenSSL versions 3.4 antérieure à 3.4.1.
- OpenSSL versions 3.3 antérieure à 3.3.3.
- OpenSSL versions 3.2 antérieure à 3.2.4.

Recommandations

Se référer au Bulletin de sécurité OpenSSL du 11 Février 2025 :
https://openssl-library.org/news/secadv/20250211.txt