



DJ-CERT

Centre national de veille,
d'alerte et de réponse aux
attaques informatiques

Autorité Nationale de Cybersécurité

Djibouti le, 20-10-2025

BULLETIN ALERTES

Objet	Multiples vulnérabilités dans OpenSSL
Référence	1405
Date de Publication	2025-10-02
Sévérité	Elevé

IMPACT :

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

SYSTÈME AFFECTÉ :

- OpenSSL versions 1.0.2x antérieures à 1.0.2zm (support payant)
- OpenSSL versions 1.1.1x antérieures à 1.1.1zd (support payant)
- OpenSSL versions 3.0.x antérieures à 3.0.18
- OpenSSL versions 3.2.x antérieures à 3.2.6
- OpenSSL versions 3.3.x antérieures à 3.3.5
- OpenSSL versions 3.4.x antérieures à 3.4.3
- OpenSSL versions 3.5.x antérieures à 3.5.4

DÉSCRIPTION :

Plusieurs vulnérabilités ont été découvertes dans OpenSSL. Elles peuvent être exploitées par un attaquant pour exécuter du code arbitraire à distance, provoquer un déni de service à distance ou compromettre la confidentialité des données.

SOLUTION :

Consulter le bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

DOCUMENTATION :

- Bulletin de sécurité OpenSSL du 30 septembre 2025

<https://openssl-library.org/news/secadv/20250930.txt>

- Référence CVE CVE-2025-9230

<https://www.cve.org/CVERecord?id=CVE-2025-9230>

- Référence CVE CVE-2025-9231

<https://www.cve.org/CVERecord?id=CVE-2025-9231>

- Référence CVE CVE-2025-9232

<https://www.cve.org/CVERecord?id=CVE-2025-9232>