

Affaire suivie par :  
CERT-FR

## AVIS DU CERT-FR

### Objet : Multiples vulnérabilités dans OpenSSL

### Gestion du document

Référence	CERTFR-2014-AVI-435
Titre	Multiples vulnérabilités dans OpenSSL
Date de la première version	16 octobre 2014
Date de la dernière version	–
Source(s)	Bulletin de sécurité OpenSSL du 15 octobre 2014
Pièce(s) jointe(s)	Aucune

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

### 1 - Risque(s)

- déni de service à distance
- atteinte à la confidentialité des données

### 2 - Systèmes affectés

- OpenSSL versions 1.0.1 à 1.0.1i
- OpenSSL versions 1.0.0 à 1.0.0n
- OpenSSL versions 0.9.8g à 0.9.8zb

### 3 - Résumé

De multiples vulnérabilités ont été corrigées dans *OpenSSL*. Elles permettent à un attaquant de provoquer un déni de service à distance et une atteinte à la confidentialité des données.

### 4 - Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

## 5 - Documentation

- Bulletin de sécurité OpenSSL du 15 octobre 2014  
[https://www.openssl.org/news/secadv\\_20141015.txt](https://www.openssl.org/news/secadv_20141015.txt)
- Référence CVE CVE-2014-3568  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3568>
- Référence CVE CVE-2014-3567  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3567>
- Référence CVE CVE-2014-3513  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3513>

## Gestion détaillée du document

**16 octobre 2014** version initiale.

---

Conditions d'utilisation de ce document : <http://cert.ssi.gouv.fr/cert-fr/apropos.html>

Dernière version de ce document : <http://cert.ssi.gouv.fr/site/CERTFR-2014-AVI-435>

---