

Affaire suivie par :  
CERT-FR

## AVIS DU CERT-FR

### Objet : Multiples vulnérabilités dans OpenSSL

### Gestion du document

Référence	CERTFR-2014-AVI-253
Titre	Multiples vulnérabilités dans OpenSSL
Date de la première version	05 juin 2014
Date de la dernière version	–
Source(s)	Bulletin de sécurité OpenSSL du 05 juin 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)

- exécution de code arbitraire à distance
- déni de service à distance
- atteinte à l'intégrité des données
- atteinte à la confidentialité des données

### 2 - Systèmes affectés

- OpenSSL 0.9.8 versions antérieures à 0.9.8za
- OpenSSL 1.0.0 versions antérieures à 1.0.0m
- OpenSSL 1.0.1 versions antérieures à 1.0.1h

### 3 - Résumé

De multiples vulnérabilités ont été corrigées dans *OpenSSL*. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, un déni de service à distance et une atteinte à l'intégrité 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 05 juin 2014  
[http://www.openssl.org/news/secadv\\_20140605.txt](http://www.openssl.org/news/secadv_20140605.txt)
- Référence CVE CVE-2010-5298  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-5298>
- Référence CVE CVE-2014-0076  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0076>
- Référence CVE CVE-2014-0195  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0195>
- Référence CVE CVE-2014-0198  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0198>
- Référence CVE CVE-2014-0221  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0221>
- Référence CVE CVE-2014-0224  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224>
- Référence CVE CVE-2014-3470  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3470>

## Gestion détaillée du document

**05 juin 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-253>

---