



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

**S . G . D . S . N**  
Agence nationale de la sécurité  
des systèmes d'information  
CERTA

Paris, le 04 mai 2011  
N° CERTA-2011-AVI-073-002

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans OpenSSL

---

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>  
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2011-AVI-073>

---

### Gestion du document

Référence	CERTA-2011-AVI-073-002
Titre	Vulnérabilité dans OpenSSL
Date de la première version	09 février 2011
Date de la dernière version	04 mai 2011
Source(s)	Avis de sécurité OpenSSL du 08 février 2011
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

Déni de service à distance.

## 2 Systèmes affectés

- OpenSSL versions 0.9.8h à 0.9.8q ;
- OpenSSL versions 1.0.0 à 1.0.0c.

## 3 Résumé

Une vulnérabilité dans OpenSSL permet à une personne malintentionnée de provoquer un déni de service à distance.

## 4 Description

Une vulnérabilité dans OpenSSL permet de provoquer un déni de service à distance en envoyant des messages spécialement conçus au serveur.

Cette faille ne concerne que les serveurs utilisant la fonction `SSL_CTX_set_tlsext_status_cb()`. Les versions 2.3.3 et suivantes du serveur Apache `httpd` sont notamment concernées.

## 5 Solution

Mettre à jour en version 1.0.0d ou en version 0.9.8r.

## 6 Documentation

- Avis de sécurité OpenSSL du 08 février 2011 :  
[http://www.openssl.org/news/secadv\\_20110208.txt](http://www.openssl.org/news/secadv_20110208.txt)
- Bulletin de sécurité Fedora FEDORA-2011-1255 du 10 février 2011 :  
<http://lists.fedoraproject.org/pipermail/package-announce/2011-March/056102.html>
- Bulletin de sécurité Fedora FEDORA-2011-1273 du 10 février 2011 :  
<http://lists.fedoraproject.org/pipermail/package-announce/2011-February/054007.html>
- Bulletin de sécurité Fedora FEDORA-2011-5865 du 23 avril 2011 (mingw32-openssl) :  
<http://lists.fedoraproject.org/pipermail/package-announce/2011-May/059313.html>
- Bulletin de sécurité Fedora FEDORA-2011-5876 du 23 avril 2011 (mingw32-openssl) :  
<http://lists.fedoraproject.org/pipermail/package-announce/2011-May/059314.html>
- Bulletin de sécurité Mandriva MDVSA-2011:028 du 15 février 2011 :  
<http://www.mandriva.com/support/security/advisories/?name=MDVSA-2011:028>
- Bulletin de sécurité Ubuntu USN-1064-1 du 15 février 2011 :  
<http://www.ubuntu.com/usn/usn-1064-1>
- Référence CVE CVE-2011-0014 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0014>

## Gestion détaillée du document

**09 février 2011** version initiale.

**16 février 2011** ajout des références aux bulletins Fedora, Mandriva et Ubuntu.

**04 mai 2011** ajout de la référence au bulletin Fedora (mingw32-openssl).