

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-2009-AVI-006>

Gestion du document

Référence	CERTA-2009-AVI-006
Titre	Vulnérabilité dans OpenSSL
Date de la première version	07 janvier 2009
Date de la dernière version	–
Source(s)	Avis de sécurité OpenSSL du 07 janvier 2009
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

Contournement de la politique de sécurité.

2 Systèmes affectés

– OpenSSL pour les versions antérieures à 0.9.8j.

3 Résumé

Une vulnérabilité a été identifiée dans OpenSSL. Elle permet à un site malveillant de contourner la vérification de la signature par le poste de l'utilisateur.

4 Description

Une vulnérabilité a été identifiée dans OpenSSL. Plusieurs fonctions ne vérifient pas correctement le retour de la fonction `EVP_VerifyFinal()` pour des signatures avec clés DSA ou ECDSA. Une mauvaise signature est alors considérée comme bonne.

Cette vulnérabilité peut être exploitée pour contourner la vérification de la signature par le client, dans le cas où la personne malveillante administre un site malveillant ou utilise une attaque de la forme homme-au-milieu.

5 Solution

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

6 Documentation

- Bulletin de sécurité OpenSSL du 07 janvier 2009 :
http://www.openssl.org/news/secadv_20090107.txt
- Référence CVE CVE-2008-5077 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5077>

Gestion détaillée du document

07 janvier 2009 version initiale.