



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 14 février 2011  
N° CERTA-2011-AVI-085

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans OpenSSH

---

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-085>

---

### Gestion du document

Référence	CERTA-2011-AVI-085
Titre	Vulnérabilité dans OpenSSH
Date de la première version	14 février 2011
Date de la dernière version	–
Source(s)	Avis de sécurité OpenSSH
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

Atteinte à la confidentialité des données.

## 2 Systèmes affectés

OpenSSH 5.7 et versions antérieures.

## 3 Résumé

Une vulnérabilité dans OpenSSH peut porter atteinte à la confidentialité des données.

## 4 Description

La version 5.8 de OpenSSH corrige une vulnérabilité pouvant porter atteinte à la confidentialité des données. Lors de la génération de certificats *legacy*, le champ *nonce* n'est pas correctement initialisé à l'aide de données aléatoires, mais contient des données issues de la pile. Ces données peuvent potentiellement contenir des informations sensibles.

## **5 Solution**

La version 5.8 de OpenSSH corrige cette vulnérabilité. Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

## **6 Documentation**

- Avis de sécurité OpenSSH :  
<http://www.openssh.com/txt/legacy-cert.adv>
- Sortie de la version 5.8 de OpenSSH :  
<http://www.openssh.com/txt/release-5.8>

## **Gestion détaillée du document**

**14 février 2011** version initiale.