



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 07 juillet 2004  
N° CERTA-2004-AVI-229

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité de nCipher netHSM

---

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-2004-AVI-229>

---

### Gestion du document

Référence	CERTA-2004-AVI-229
Titre	Vulnérabilité de nCipher netHSM
Date de la première version	07 juillet 2004
Date de la dernière version	–
Source(s)	Bulletin de sécurité nCipher n° 10
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

Divulgarion d'informations sensibles.

## 2 Systèmes affectés

- nCipher netHSM version 2 ;
- nCipher netHSM version 2.1.

## 3 Résumé

Une vulnérabilité présente dans nCipher netHSM permet à un utilisateur local d'accéder à des informations sensibles.

## 4 Description

NetHSM (Network Connected Hardware Security Modules) est un équipement connecté au réseau utilisé pour le stockage de clés cryptographiques qui fournit des fonctions de signature, chiffrement et déchiffrement.

Une vulnérabilité permet à un utilisateur local mal intentionné de récupérer la phrase d'authentification (*passphrase*) sauvegardée en clair dans un fichier journal.

## **5 Solution**

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation). Cette action étant irréversible, il est conseillé de contacter le support nCipher en cas de doute.

## **6 Documentation**

Bulletin de sécurité nCipher numéro 10 du 22 juin 2004 :  
<http://www.ncipher.com/support/advisories/advisory10.htm>

## **Gestion détaillée du document**

**07 juillet 2004** version initiale.