



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 26 février 2004
N° CERTA-2004-AVI-049

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans nCipher

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-049>

Gestion du document

Référence	CERTA-2004-AVI-049
Titre	Vulnérabilité dans nCipher
Date de la première version	26 février 2004
Date de la dernière version	–
Source(s)	Avis de Sécurité nCipher N°9
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

Divulgateion de données sensibles.

2 Systèmes affectés

- module de deuxième génération (nCxxx2W ou nCxxx2P), avec une version du progiciel postérieure à 1.67.0 et antérieure à 2.0.0 ;
- module de deuxième génération (nCxxx2W ou nCxxx2P), avec une version du progiciel postérieure à 2.0.0, et le dispositif *generalSEE* activé ou potentiellement activé ;
- module de troisième génération (nCxxx3S ou nCxxx3P), avec une version du progiciel postérieure à 2.12.0, et le dispositif *generalSEE* activé ou potentiellement activé.

3 Description

A cause d'une erreur d'implémentation dans certaines versions du progiciel de nCipher, un utilisateur mal intentionné pouvant exécuter certaines commandes sur un HSM (Hardware Security Module), pourra récupérer des informations sensibles dans la mémoire d'exécution, telles que, par exemple, les clefs secrètes utilisées par le module.

4 Solution

L'entreprise nCipher conseille de mettre le progiciel à jour. La mise à jour du progiciel peut être envoyée par le support technique, dont les coordonnées se trouvent sur l'avis d'origine de nCipher.

<http://www.ncipher.com/support/advisories/advisory9.htm>

5 Documentation

Avis de sécurité n°9 de nCipher

<http://www.ncipher.com/support/advisories/advisory9.htm>

Gestion détaillée du document

26 février 2004 version initiale.