Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 08 octobre 2010
N° CERTA-2010-AVI-478

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans RSA Authentication Client

Gestion du document

Référence	CERTA-2010-AVI-478
Titre	Vulnérabilité dans RSA Authentication Client
Date de la première version	08 octobre 2010
Date de la dernière version	–
Source(s)	Bulletin du NIST CVE-2010-3321
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

RSA Authentication Client, versions 2.x, 3.x, 3.5.x. utilisé avec un appareil RSA SecurID 800.

3 Résumé

Une vulnérabilité dans RSA Authentication Client est exploitable par un utilisateur malveillant pour contourner la politique de sécurité.

4 Description

Un gestion défaillante des marqueurs `SENSITIVE` et `NON-EXTRACTABLE` permet à un utilisateur malveillant de récupérer les clefs secrètes par le biais de l'API PKCS#11.

5 Solution

La version RSA Client Authentication 3.5.3 corrige cette erreur.
Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Site de l'éditeur RSA :
  http://www.rsa.com/
- Bulletin du NIST CVE-2010-3321 du 06 octobre 2010 :
  http://nvd.nist.gov/nvd.cfm?cvename=CVE-2010-3321
- Référence CVE CVE-2010-3321 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3321

Gestion détaillée du document

08 octobre 2010 version initiale.