

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité des produits RSA

---

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-2007-AVI-317>

---

### Gestion du document

Référence	CERTA-2007-AVI-317
Titre	Vulnérabilité des produits RSA
Date de la première version	18 juillet 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité TippingPoint du 12 juillet 2007
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

Exécution de code arbitraire à distance.

## 2 Systèmes affectés

- RSA SecureID Appliance 2.x ;
- RSA ACE/Server 5.x ;
- RSA Authentication Manager 6.x.

## 3 Description

Une vulnérabilité dans les produits RSA permet à un utilisateur distant malintentionné d'exécuter du code arbitraire sur le système vulnérable.

## 4 Solution

Se référer aux bulletins de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation) :  
– Pour RSA SecureID Appliance :

- [http://knowledge.rsasecurity.com/dlcpages/rsa\\_secureid/secureid\\_dlc\\_app.asp](http://knowledge.rsasecurity.com/dlcpages/rsa_secureid/secureid_dlc_app.asp)
- Pour RSA ACE/Server :  
[http://knowledge.rsasecurity.com/dlcpages/rsa\\_secureid/secureid\\_dlc\\_as52p.asp](http://knowledge.rsasecurity.com/dlcpages/rsa_secureid/secureid_dlc_as52p.asp)
- Pour RSA Authentication Manager :  
[http://knowledge.rsasecurity.com/dlcpages/rsa\\_secureid/secureid\\_dlc\\_am60p2.asp](http://knowledge.rsasecurity.com/dlcpages/rsa_secureid/secureid_dlc_am60p2.asp)

## **5 Documentation**

Bulletin de sécurité TippingPoint du 12 juillet 2007 :  
<http://dvlabs.tippingpoint.com/advisory/TPTI-07-12>

### **Gestion détaillée du document**

**18 juillet 2007** version initiale.