

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans RSA Federated Identity Manager

---

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-2010-AVI-334>

---

### Gestion du document

Référence	CERTA-2010-AVI-334
Titre	Vulnérabilité dans RSA Federated Identity Manager
Date de la première version	22 juillet 2010
Date de la dernière version	–
Source(s)	Avis EMC RSA ESA-2010-011 du 20 juillet 2010
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 ;
- injection de requêtes illégitime par rebond.

## 2 Systèmes affectés

RSA Federated Identity Manager versions 4.0 et 4.1.

## 3 Résumé

Une vulnérabilité dans le produit RSA Federated Identity Manager peut être exploitée par un utilisateur malveillant afin de rediriger un utilisateur légitime du système vers un site non souhaité.

## 4 Description

Une vulnérabilité dans le produit RSA Federated Identity Manager peut être exploitée afin de rediriger un utilisateur légitime vers un site Web arbitraire, choisi par l'attaquant. Il est par exemple possible de rediriger les utilisateurs vers un faux site.

## **5 Solution**

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

## **6 Documentation**

- Référence CVE CVE-2010-2337 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2337>
- Avis EMC RSA ESA-2010-011 du 20 juillet 2010 :  
<http://archives.neohapsis.com/archives/bugtraq/2010-07/0187.html>
- Information sur le produit RSA Federated Identity Manager :  
<http://www.rsa.com/node.aspx?id=1191>

## **Gestion détaillée du document**

**22 juillet 2010** version initiale.