

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans EMC RSA BSAFE

---

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-2013-AVI-367>

---

### Gestion du document

Référence	CERTA-2013-AVI-367
Titre	Multiples vulnérabilités dans EMC RSA BSAFE
Date de la première version	20 juin 2013
Date de la dernière version	–
Source(s)	Bulletin de sécurité EMC ESA-2013-032 du 19 juin 2013 Bulletin de sécurité EMC ESA-2013-039 du 19 juin 2013 Bulletin de sécurité EMC ESA-2013-045 du 19 juin 2013
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(s)

- atteinte à la confidentialité des données

## 2 Systèmes affectés

- RSA BSAFE SSL-C versions antérieures à 2.8.7
- RSA BSAFE SSL-J versions antérieures à 6.0.1
- RSA BSAFE SSL-J versions antérieures à 5.1.2
- RSA BSAFE Micro Edition Suite versions antérieures à 4.0.3
- RSA BSAFE Micro Edition Suite versions antérieures à 3.2.5

## 3 Résumé

De multiples vulnérabilités ont été corrigées dans *EMC RSA BSAFE*. Elles permettent à un attaquant de provoquer une atteinte à la confidentialité des données.

## 4 Solution

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

## 5 Documentation

- Bulletin de sécurité EMC ESA-2013-032 du 19 juin 2013  
<http://archives.neohapsis.com/archives/bugtraq/2013-06/att-0067/ESA-2013-032.txt>
- Bulletin de sécurité EMC ESA-2013-039 du 19 juin 2013  
<http://archives.neohapsis.com/archives/bugtraq/2013-06/att-0066/ESA-2013-039.txt>
- Bulletin de sécurité EMC ESA-2013-045 du 19 juin 2013  
<http://archives.neohapsis.com/archives/bugtraq/2013-06/att-0065/ESA-2013-045.txt>
- Référence CVE CVE-2013-0169  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0169>
- Référence CVE CVE-2011-3389  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3389>

## Gestion détaillée du document

**20 juin 2013** version initiale.