Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 septembre 2012
N° CERTA-2012-AVI-498

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans RSA BSAFE SSL-C

Gestion du document

Référence	CERTA-2012-AVI-498
Titre	Vulnérabilités dans RSA BSAFE SSL-C
Date de la première version	13 septembre 2012
Date de la dernière version	–
Source(s)	Bulletin de sécurité ESA-2012-029 du 11 septembre 2012
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 ;
- déni de service à distance ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

Toutes les versions de RSA BSAFE SSL-C antérieures à 2.8.6.

3 Résumé

Plusieurs vulnérabilités ont été corrigées dans *RSA BSAFE SSL-C*. Elles concernent une atteinte à la confidentialité des données, un déni de service et éventuellement une exécution de code arbitraire à distance.

4 Solution

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

5 Documentation

- Bulletin de sécurité ESA-2012-029 du 11 septembre 2012 :
  http://archives.neohapsis.com/archives/bugtraq/2012-09/att-0046/ESA-2012-029.txt
- Référence CVE CVE-2011-3389 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3389
- Référence CVE CVE-2012-2110 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2110
- Référence CVE CVE-2012-2131 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2131

Gestion détaillée du document

13 septembre 2012 version initiale.