Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 21 mars 2012
N° CERTA-2012-AVI-162

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans RSA enVision

Gestion du document

Référence	CERTA-2012-AVI-162
Titre	Multiples vulnérabilités dans RSA enVision
Date de la première version	21 mars 2012
Date de la dernière version	–
Source(s)	Bulletin de sécurité ESA-2012-014
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

– Versions antérieures à RSA enVision 4.1 Patch 4.

3 Résumé

De multiples vulnérabilités ont été corrigées dans *RSA enVision*. L'exploitation de ces vulnérabilités pouvait conduire à une prise de contrôle du serveur à distance.

4 Description

Les correctifs concernent cinq vulnérabilités :

– la présence d'identifiants inscrits en dur dans le code ;
– plusieurs « injections SQL » ;

- un parcours arbitraire des répertoires ;
- une restriction inappropriée lors de nombreuses tentatives de connexion ;
- plusieurs injections de code dites *XSS*.

5 Solution

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

6 Documentation

- Référence EMC ESA-2012-014 :
  http://archives.neohapsis.com/archives/bugtraq/2012-03/att-0081/ESA-2012-014.txt
- Référence CVE CVE-2012-0399 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0399
- Référence CVE CVE-2012-0400 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0400
- Référence CVE CVE-2012-0401 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0401
- Référence CVE CVE-2012-0402 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0402
- Référence CVE CVE-2012-0403 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0403

Gestion détaillée du document

21 mars 2012 version initiale.