Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 23 janvier 2008
N° CERTA-2008-AVI-035

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités des produits IBM

Gestion du document

Référence	CERTA-2008-AVI-035
Titre	Multiples vulnérabilités des produits IBM
Date de la première version	23 janvier 2008
Date de la dernière version	–
Source(s)	Mises à jour de sécurité IBM
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

- Déni de service à distance ;
- atteinte à l'intégrité des données ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

- IBM Tivoli Provisioning Manager for OS Deployment 5.x ;
- IBM Tivoli Business Service Manager 4.x ;
- IBM Websphere Business Modeler 6.x ;
- IBM Websphere Application Server 6.0.X.

3 Résumé

Plusieurs vulnérabilités ont été découvertes dans des produits IBM. L'exploitation de ces vulnérabilités permet de provoquer un déni de service ou d'effectuer des actions malveillantes sur le système de fichiers de la machine cible.

4 Description

Plusieurs vulnérabilités ont été découvertes dans des produits IBM :

- une vulnérabilité dans l'applicatif IBM Tivoli Provisioning Manager for OS Deployment permet à un utilisateur malintentionné d'effectuer un déni de service depuis le réseau local ;
- une vulnérabilité dans l'applicatif IBM Tivoli Business Service Manager permet de récupérer des mots de passes stockés en clair ;
- une vulnérabilité dans l'applicatif IBM Websphere Business Modeler permet à un utilisateur légitime malintentionné d'effacer des données importantes ne lui appartenant pas.
- D'autres vulnérabilités dont l'impact n'a pas été spécifié par IBM ont été découvertes dans IBM Websphere Application Server.

5 Solution

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

6 Documentation

- Bulletin de sécurité IBM swg24018010 du 23 janvier 2008 :
  http://www-1.ibm.com/support/docview.wss?uid=swg24018010
- Bulletin de sécurité IBM swg24017939 du 23 janvier 2008 :
  http://www-1.ibm.com/support/docview.wss?uid=swg24017939
- Bulletin de sécurité IBM swg24018060 du 23 janvier 2008 :
  http://www-1.ibm.com/support/docview.wss?uid=swg24018060
- Bulletin de sécurité IBM swg24018061 du 23 janvier 2008 :
  http://www-1.ibm.com/support/docview.wss?uid=swg24018061
- Bulletin de sécurité IBM swg27006876 du 23 janvier 2008 :
  http://www-1.ibm.com/support/docview.wss?uid=swg27006876
- Référence CVE CVE-2008-0389 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0389
- Référence CVE CVE-2008-0401 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0401
- Référence CVE CVE-2008-0402 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0402

Gestion détaillée du document

23 janvier 2008 version initiale.