



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 30 janvier 2008
N° CERTA-2008-AVI-040

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans IBM Informix

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-2008-AVI-040>

Gestion du document

Référence	CERTA-2008-AVI-040
Titre	Multiples vulnérabilités dans IBM Informix
Date de la première version	30 janvier 2008
Date de la dernière version	–
Source(s)	Bulletin IBM 21294211 du 28 janvier 2008
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

IBM Informix Dynamic Server 10.x et 11.x, sur *Microsoft Windows*.

3 Résumé

Plusieurs vulnérabilités dans *Informix* permettent à un utilisateur malveillant d'exécuter du code arbitraire à distance avec des droits d'administrateur.

4 Description

Les modules RPC d'*Informix Storage Manager* utilisent une bibliothèque XDR (couche présentation).

La bibliothèque utilisée sur les systèmes *Microsoft Windows* présente plusieurs vulnérabilités permettant de provoquer des débordements de mémoire. L'exploitation de ces vulnérabilités, par le biais de requêtes malformées,

permet à un utilisateur malveillant d'exécuter du code arbitraire à distance avec les droits d'administration sur la machine.

Sur les systèmes Unix, la bibliothèque XDR utilisée est celle du système d'exploitation. Elle n'est pas concernée par les vulnérabilités ci-dessus.

5 Solution

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

6 Documentation

- Bulletin de sécurité IBM swg21294211 du 28 janvier 2008 :
<http://www-1.ibm.com/support/docview.wss?uid=swg21294211>

Gestion détaillée du document

30 janvier 2008 version initiale.