

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans IBM Informix Dynamic Server

---

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-155>

---

### Gestion du document

Référence	CERTA-2008-AVI-155
Titre	Multiples vulnérabilités dans IBM Informix Dynamic Server
Date de la première version	20 mars 2008
Date de la dernière version	–
Source(s)	Bulletins 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

- Exécution de code arbitraire à distance ;
- déni de service à distance.

## 2 Systèmes affectés

- IBM Informix Dynamic Server 7.x ;
- IBM Informix Dynamic Server 9.x ;
- IBM Informix Dynamic Server 10.x ;
- IBM Informix Dynamic Server 11.x.

## 3 Résumé

Plusieurs vulnérabilités ont été découvertes dans IBM Informix Dynamic Server permettant à un individu malveillant d'effectuer un déni de service ou une exécution de code arbitraire à distance.

## 4 Description

De multiples vulnérabilités dans IBM Informix Dynamic Server ont été découvertes :

- une erreur non spécifiée dans la gestion des demandes de connexion malformée peut être exploitée via un paquet spécialement conçu ;
- une erreur dans *oinit.exe* lors de l'utilisation de la variable *DBPATH* pendant l'authentification permet à une personne malintentionnée de provoquer un déni de service via une variable *DBPATH* trop longue envoyée au port par défaut *1526/TCP* ;
- une erreur dans le fichier *oinit.exe* permet un dépassement de mémoire tampon via l'envoi, pendant le processus d'authentification, d'un mot de passe trop long sur le port par défaut *1526/TCP*.

## 5 Solution

Se référer aux bulletins de sécurité IBM pour l'obtention des correctifs (cf. section Documentation).

## 6 Documentation

- Bulletin de sécurité IBM swg1IC55207 du 20 mars 2008 :  
<http://www-1.ibm.com/support/docview.wss?uid=swg1IC55207>
- Bulletin de sécurité IBM swg1IC55208 du 20 mars 2008 :  
<http://www-1.ibm.com/support/docview.wss?uid=swg1IC55208>
- Bulletin de sécurité IBM swg1IC55209 du 20 mars 2008 :  
<http://www-1.ibm.com/support/docview.wss?uid=swg1IC55209>
- Bulletin de sécurité IBM swg1IC55209 du 20 mars 2008 :  
<http://www-1.ibm.com/support/docview.wss?uid=swg1IC55209>
- Bulletin de sécurité IBM swg1IC55210 du 20 mars 2008 :  
<http://www-1.ibm.com/support/docview.wss?uid=swg1IC55210>
- Bulletin de sécurité IBM swg1IC55224 du 20 mars 2008 :  
<http://www-1.ibm.com/support/docview.wss?uid=swg1IC55224>
- Bulletin de sécurité IBM swg1IC55225 du 20 mars 2008 :  
<http://www-1.ibm.com/support/docview.wss?uid=swg1IC55225>
- Référence CVE CVE-2008-0727 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0727>
- Référence CVE CVE-2008-0949 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0949>

## Gestion détaillée du document

20 mars 2008 version initiale.