Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 05 août 2006
N° CERTA-2006-AVI-334

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans IBM Informix Dynamic Server (IDS)

Gestion du document

Référence	CERTA-2006-AVI-334
Titre	Multiples vulnérabilités dans IBM Informix Dynamic Server (IDS)
Date de la première version	05 août 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité IBM du 31 juillet 2006
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 ;
- contournement de la politique de sécurité ;
- atteinte à l'intégrité des données ;
- atteinte à la confidentialité des données ;
- élévation de privilèges.

2 Systèmes affectés

- IBM Informix Dynamic Server (IDS) version 7.31.xD8 ainsi que celles antérieures ;
- IBM Informix Dynamic Server (IDS) version 9.40.xC5 ainsi que celles antérieures ;
- IBM Informix Dynamic Server (IDS) version 10.00.xC3 ainsi que celles antérieures.

3 Résumé

Plusieurs vulnérabilités ont été découvertes dans le logiciel `Informix Dynamic Server` (IDS) d'IBM. Elles permettraient sous certaines conditions à un attaquant distant ou un utilisateur local d'exécuter du code arbitraire, de provoquer un déni de service ou d'accéder à des informations sensibles sur un système vulnérable.

4 Description

Plusieurs vulnérabilités ont été identifiées dans le logiciel `Informix Dynamic Server` (IDS) d'IBM. Parmi-celles-ci :

- débordement de tampon possible au moyen de certaines fonctions comme `DBINFO()`, `LOTOFILE()`, `FILETOCLOB()`, `getname()` ou `ifx_file_to_file()` ;
- stockage de mots de passe utilisateurs en clair dans la mémoire partagée ;
- défaut de permission pour créer une base de donnéees ;
- gestion non correcte de certaines variables d'environnement comme SQLIDEBUG.

Ces vulnérabilités permettraient à un attaquant malveillant d'exécuter du code arbitraire ou de provoquer un déni de service (DoS) sur un système vulnérable, ou bien encore d'augmenter ses privilèges et d'accéder à des informations sensibles sur le système.

5 Solution

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

6 Documentation

Bulletin de sécurité 1242921 d'IBM du 31 juillet 2006 :
http://www-1.ibm.com/support/docview.wss?uid=swg2242921

Gestion détaillée du document

05 août 2006 version initiale.