

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité sur Sybase Adaptive 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-2002-AVI-258>

Gestion du document

Référence	CERTA-2002-AVI-258
Titre	Vulnérabilités sur Sybase Adaptive Server
Date de la première version	04 décembre 2002
Date de la dernière version	–
Source(s)	Liste de diffusion Bugtraq
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 ;
- déni de service.

2 Systèmes affectés

Sybase Adaptive Server versions 12.0 et 12.5.

3 Résumé

Plusieurs débordements de pile présents sur Sybase Adaptive Server permettent à un utilisateur mal intentionné d'exécuter du code arbitraire ou de réaliser un déni de service à distance.

4 Description

Sybase Adaptive Server est un gestionnaire de bases de données. Plusieurs débordements de pile sont présents sur les fonctions et les procédures stockées étendues (ESP).

La première vulnérabilité concerne la procédure stockée étendue `xp_freedll`, chargée de libérer une bibliothèque DLL chargée par une autre procédure. Le nom de la bibliothèque à libérer est utilisé comme paramètre d'entrée dans la procédure `xp_freedll`.

La seconde vulnérabilité concerne la fonction `DBCC CHECK_VERIFY`. Cette fonction est utilisée pour vérifier le résultat de la fonction `DBCC CHECKSTORAGE` chargée de rapporter les erreurs constatées durant le contrôle des bases de données. Le nom de la base de données à vérifier est utilisé comme paramètre d'entrée de la fonction `DBCC CHECK_VERIFY`.

La dernière vulnérabilité concerne la fonction `DROP DATABASE` qui permet de supprimer une base de données sur le serveur. Le nom de la base de données à supprimer est utilisé comme paramètre d'entrée dans la fonction `DROP DATABASE`.

L'absence de vérification de la longueur des noms utilisés comme paramètre pour les fonctions et la procédure ci-dessus permet à un utilisateur mal intentionné d'exécuter un code arbitraire.

Ces trois vulnérabilités ne sont exploitables que localement.

5 Solution

Appliquer les correctifs disponibles sur le site de l'éditeur (voir section documentation).

6 Documentation

- Avis de sécurité d'Application Security Inc. sur `DBCC CHECK_VERIFY`
<http://www.appsecinc.com/resources/alerts/sybase/02-0001.html>
- Avis de sécurité d'Application Security Inc. sur `DROP DATABASE`
<http://www.appsecinc.com/resources/alerts/sybase/02-0002.html>
- Avis de sécurité d'Application Security Inc. sur `xp_freedll`
<http://www.appsecinc.com/resources/alerts/sybase/02-0003.html>

Gestion détaillée du document

04 décembre 2002 version initiale.