



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 14 novembre 2003
N° CERTA-2003-AVI-188-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité sur Postgresql

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-2003-AVI-188>

Gestion du document

Référence	CERTA-2003-AVI-188-001
Titre	Vulnérabilité sur Postgresql
Date de la première version	12 novembre 2003
Date de la dernière version	14 novembre 2003
Source(s)	Buletin de sécurité Debian DSA 397-1
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

Postgresql versions antérieures à la version 7.3.4.

3 Résumé

Une vulnérabilité présente sur Postgresql permet à un utilisateur mal intentionné d'exécuter du code arbitraire sur la machine hébergeant le serveur Postgresql.

4 Description

Un débordement de mémoire présent dans la fonction de conversion `to_ascii` de Postgresql permet à un utilisateur mal intentionné d'exécuter du code arbitraire sur la machine hébergeant ce service.

5 Solution

Appliquer le correctif correspondant à votre système (cf section documentation).

6 Documentation

- Avis de sécurité Debian DSA-397-1 :
<http://www.debian.org/security/2003/dsa.397.html>
- Avis de sécurité Mandrake MDKSA-2003:102 :
<http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2003:102>
- Avis de sécurité RedHat RHSA-2003:313-10 :
<https://rhn.redhat.com/errata/RHSA-2003-313.html>
- Référence CVE : CAN-2003-0901 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0901>

Gestion détaillée du document

12 novembre 2003 version initiale.

14 novembre 2003 ajout du bulletin de sécurité RedHat Linux.