



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 21 avril 2005
N° CERTA-2005-AVI-049-008

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de 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-2005-AVI-049>

Gestion du document

Référence	CERTA-2005-AVI-049-008
Titre	Vulnérabilité de PostgreSQL
Date de la première version	09 février 2005
Date de la dernière version	21 avril 2005
Source(s)	Bulletin de sécurité Debian DSA-668
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

- Contournement de la politique de sécurité ;
- exécution locale de code arbitraire avec les droits du serveur PostgreSQL.

2 Systèmes affectés

- Pour la branche 7.2.x, PostgreSQL versions 7.2.6 et antérieures ;
- pour la branche 7.3.x, PostgreSQL versions 7.3.8 et antérieures ;
- pour la branche 7.4.x, PostgreSQL versions 7.4.6 et antérieures ;
- pour la branche 8.0.x, PostgreSQL versions 8.0.0 et antérieures.

3 Description

PostgreSQL est un outil de base de données Open Source.

Plusieurs vulnérabilités permettent à un utilisateur mal intentionné de contourner les vérifications de sécurité ou d'exécuter du code arbitraire, en local, avec les droits du serveur PostgreSQL.

4 Solution

Dans tous les cas, se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

Mettre à jour PostgreSQL en versions 8.0.1, 7.4.7, 7.3.9 ou 7.2.7.

PostgreSQL est téléchargeable à l'adresse suivante :

<http://wwwmaster.postgresql.org/download/mirror-ftp/>

5 Documentation

- Site Internet de PostgreSQL :
<http://www.postgresql.org>
- Annonce de la vulnérabilité :
<http://archives.postgresql.org/pgsql-bugs/2005-01/msg00269.php>
- Annonce des nouvelles versions de PostgreSQL corrigeant la vulnérabilité :
<http://archives.postgresql.org/pgsql-announce/2005-02/msg00000.php>
- Bulletin de sécurité Debian DSA-668 du 04 février 2005 :
<http://www.debian.org/security/2005/dsa-668>
- Bulletin de sécurité Debian DSA-683 du 15 février 2005 :
<http://www.debian.org/security/2005/dsa-683>
- Bulletin de sécurité Gentoo GLSA 200502-08 du 07 février 2005 :
<http://www.gentoo.org/security/en/glsa/glsa-200502-08.xml>
- Bulletin de sécurité Gentoo GLSA 200502-19 du 14 février 2005 :
<http://www.gentoo.org/security/en/glsa/glsa-200502-19.xml>
- Bulletin de sécurité OpenBSD pour postgresql-server du 05 février 2005 :
<http://www.vuxml.org/openbsd/>
- Bulletin de sécurité FreeBSD pour ja-postgresql, postgresql, postgresql-server et postgresql-devel du 08 février 2005 :
<http://www.vuxml.org/freebsd/>
- Bulletin de sécurité FreeBSD pour ja-postgresql, postgresql et postgresql-server du 17 février 2005 :
<http://www.vuxml.org/freebsd/>
- Mise à jour de sécurité des paquetages NetBSD postgresql73, postgresql74 et postgresql80 :
<ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/databases/postgresql73/README.html>
<ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/databases/postgresql74/README.html>
<ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/databases/postgresql80/>
- Bulletin de sécurité RedHat RHSA-2005:138 du 15 février 2005 :
<http://rhn.redhat.com/errata/RHSA-2005-138.html>
- Bulletin de sécurité RedHat RHSA-2005:141 du 14 février 2005 :
<http://rhn.redhat.com/errata/RHSA-2005-141.html>
- Bulletin de sécurité RedHat RHSA-2005:150 du 16 février 2005 :
<http://rhn.redhat.com/errata/RHSA-2005-150.html>
- Bulletin de sécurité Mandrake MDKSA-2005:040 du 17 février 2005 :
<http://www.mandrakesoft.com/security/advisories?name=MDKSA-2005:040>
- Mise à jour de sécurité Fedora Core 2 pour PostgreSQL :
<http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/>
- Mise à jour de sécurité Fedora Core 3 pour PostgreSQL :
<http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/>
- Bulletin de sécurité SUSE SUSE-SA:2005:027 du 20 avril 2005 :
http://www.novell.com/linux/security/advisories/2005_27_postgresql.html
- Référence CVE CAN-2005-0227 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0227>
- Référence CVE CAN-2005-0244 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0244>

- Référence CVE CAN-2005-0245 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0245>
- Référence CVE CAN-2005-0246 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0246>
- Référence CVE CAN-2005-0247 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0247>

Gestion détaillée du document

09 février 2005 version initiale.

14 février 2005 ajout de la référence au bulletin de sécurité RedHat RHSA-2005:141 et des références CVE CAN-2005-244, CAN-2005-245, CAN-2005-246 et CAN-2005-247.

15 février 2005 ajout de la référence au bulletin de sécurité Gentoo GLSA 200502-19.

16 février 2005 ajout de la référence au bulletin de sécurité Debian DSA-683.

17 février 2005 ajout de la référence au bulletin de sécurité RedHat RHSA-2005:150.

18 février 2005 ajout des références aux bulletins de sécurité Mandrake MDKSA-2005:040 et FreeBSD.

18 février 2005 ajout de la référence au bulletin de sécurité RedHat RHSA-2005:138.

28 février 2005 ajout des références aux mises à jour de sécurité Fedora pour PostgreSQL.

21 avril 2005 ajout référence au bulletin de sécurité SuSE.