



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 15 juillet 2010
N° CERTA-2010-AVI-214-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans 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-2010-AVI-214>

Gestion du document

Référence	CERTA-2010-AVI-214-002
Titre	Multiples vulnérabilités dans PostgreSQL
Date de la première version	18 mai 2010
Date de la dernière version	15 juillet 2010
Source(s)	Avis de sécurité de PostgreSQL du 14 mai 2010
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 ;
- contournement de la politique de sécurité ;
- atteinte à l'intégrité des données ;
- atteinte à la confidentialité des données ;
- élévation de privilèges.

2 Systèmes affectés

Les versions 7.4, 8.0, 8.1, 8.2, 8.3 et 8.4 de PostgreSQL sont affectées.

3 Résumé

Des vulnérabilités multiples affectent PostgreSQL et permettent à un utilisateur malveillant d'exécuter du code arbitraire, de contourner la politique de sécurité ou d'élever ses privilèges.

4 Description

Plusieurs vulnérabilités sont présentes dans PostgreSQL :

- Le module PL/Perl, s'il est installé et activé, peut permettre l'exécution de code PERL arbitraire sur le serveur ;
- Le module PL/Tcl, s'il est installé et activé, peut permettre l'exécution de code Tcl arbitraire sur le serveur.

D'autres vulnérabilités non spécifiées affectent aussi les versions vulnérables de PostgreSQL.

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation). Les versions 8.4.4, 8.3.11, 8.2.17, 8.1.21, 8.0.25 et 7.4.29 corrigent ces problèmes.

6 Documentation

- Bulletin de sécurité de l'éditeur PostgreSQL :
<http://www.postgresql.org/about/news.1203>
- Bulletin de sécurité Debian DSA-22051-1 du 24 mai 2010 :
<http://www.debian.org/security/2010/dsa-2051>
- Bulletins de sécurité Sun Solaris du 15 juillet 2010 :
http://blogs.sun.com/security/entry/cve_2010_1169_cve_2010
http://blogs.sun.com/security/entry/cve_2010_1169_cve_20101
- Référence CVE CVE-2010-1447 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1447>
- Référence CVE CVE-2010-1169 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1169>
- Référence CVE CVE-2010-1170 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1170>

Gestion détaillée du document

18 mai 2010 version initiale ;

25 mai 2010 ajout du bulletin de sécurité Debian ;

15 juillet 2010 ajout des bulletins de sécurité Sun Solaris.