



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 13 janvier 2010  
N° CERTA-2010-AVI-003-001

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans PowerDNS

---

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-003>

---

### Gestion du document

Référence	CERTA-2010-AVI-003-001
Titre	Multiples vulnérabilités dans PowerDNS
Date de la première version	07 janvier 2010
Date de la dernière version	13 janvier 2010
Source(s)	Avis de sécurité PowerDNS 2010-01 et 2010-02 du 6 janvier 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 à distance ;
- contournement de la politique de sécurité ;
- déni de service à distance.

## 2 Systèmes affectés

Les versions de PowerDNS 3.1.7.1 et les versions précédentes.

## 3 Résumé

Deux vulnérabilités dans PowerDNS Recursor permettant l'exécution de code arbitraire à distance et le contournement de la politique de sécurité ont été corrigées.

## 4 Description

Deux vulnérabilités dans PowerDNS Recursor ont été corrigées. La première permet à une personne mal-intentionnée distante de provoquer un déni de service ou d'exécuter du code arbitraire au moyen d'un paquet

spécialement réalisé. La seconde est exploitable au moyen d'une *Zone* spécialement mise en place afin de tromper PowerDNS Recursor pour qu'il accepte des données malveillantes à destination des utilisateurs du service.

## 5 Solution

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

## 6 Documentation

- Bulletins de sécurité PowerDNS 2010-01 et 2010-02 du 6 janvier 2010 :  
<http://doc.powerdns.com/powerdns-advisory-2010-01.html>  
<http://doc.powerdns.com/powerdns-advisory-2010-02.html>
- Bulletin de sécurité Debian DSA 1968-1 du 08 janvier 2010 :  
<http://list.debian.org/debian-security-announce/2010/msg00003.html>
- Référence CVE CVE-2009-4009 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-4009>
- Référence CVE cve-2009-4010 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2009-4010>

## Gestion détaillée du document

**07 janvier 2010** version initiale.

**13 janvier 2010** Ajout de la référence au bulletin de sécurité Debian.