

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité 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-2012-AVI-016>

Gestion du document

Référence	CERTA-2012-AVI-016
Titre	Vulnérabilité dans PowerDNS
Date de la première version	13 janvier 2012
Date de la dernière version	–
Source(s)	Bulletin de sécurité PowerDNS Authoritative Server du 10 janvier 2012
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

Déni de service à distance.

2 Systèmes affectés

- PowerDNS Authoritative Server versions 2.x inférieures à la 2.9.22.5 ;
- PowerDNS Authoritative Server versions 3.x inférieures à la 3.0.1.

3 Résumé

Un attaquant peut réaliser un déni de service à distance à l'aide de paquets UDP spécialement conçus.

4 Description

Une erreur dans le traitement des paquets « réponse DNS » par PowerDNS permet à un attaquant, au moyen de paquets UDP spécialement conçus, d'épuiser les ressources systèmes en forçant le serveur à répondre en boucle à ses propres réponses.

5 Solution

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

6 Documentation

- Bulletin de sécurité PowerDNS Authoritative Server du 10 janvier 2012 :
<http://www.powerdns.com/news/powerdns-security-advisory-2012-01.html>
- Référence CVE CVE-2012-0206 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0206>

Gestion détaillée du document

13 janvier 2012 version initiale.