

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Mauvais support du protocole DNS

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-181>

Gestion du document

Référence	CERTA-2005-AVI-181
Titre	Mauvais support du protocole DNS
Date de la première version	27 mai 2005
Date de la dernière version	–
Source(s)	Avis de sécurité 589088 du NISCC
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.

2 Systèmes affectés

- Serveur mandataire (« proxy ») cache *Delegate* jusqu'à la version 8.10.2 ;
- Cache DNS *DNRD* en version antérieure à la 2.18 ;
- Serveur DNS *PowerDNS* jusqu'à la version 2.9.16 ;
- Plusieurs équipements Cisco (voir avis CERTA-2005-AVI-175).

3 Description

Une mauvaise gestion de la décompression des messages DNS peut conduire à l'épuisement des ressources disponibles pour le serveur et entraîner un déni de service.

4 Solution

Se référer aux sites des constructeurs pour l'obtention du correctif (cf. Documentation).

5 Documentation

- Bulletin de sécurité 589088 du NISCC :
<http://www.niscc.gov.uk/niscc/docs/re-20050524-00432.pdf>
- Site de *delegate* :
<http://www.delegate.org>
- Site de *DNRD* :
<http://dnrd.sourceforge.net/>
- Site de *PowerDNS* :
<http://www.powerdns.com>
- Avis "Vulnérabilité du DNS de plusieurs produits Cisco" du 25 mai 2005 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-AVI-175/index.html>
- Référence CVE CAN-2005-0036 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0036>
- Référence CVE CAN-2005-0037 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0037>
- Référence CVE CAN-2005-0038 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0038>

Gestion détaillée du document

27 mai 2005 version initiale.