

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de la bibliothèque Perl Net::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-2008-AVI-144>

Gestion du document

Référence	CERTA-2008-AVI-144
Titre	Vulnérabilité de la bibliothèque Perl Net::DNS
Date de la première version	19 mars 2008
Date de la dernière version	–
Source(s)	Rapport de bogue Buzilla RedHat 426437
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

Les versions de la bibliothèque Perl Net::DNS antérieures à 0.63.

3 Résumé

Une vulnérabilité a été identifiée dans la bibliothèque Perl Net::DNS. Une personne pourrait profiter de cette dernière en construisant et en envoyant une réponse DNS construite de manière particulière, afin de perturber à distance le système vulnérable.

4 Description

Une vulnérabilité a été identifiée dans la bibliothèque Perl Net::DNS, et plus précisément dans le fichier Net/DNS/RR/A.pm. Il y aurait un mauvais contrôle effectué sur la taille d'une adresse IP. Cette bibliothèque peut être nécessaire au fonctionnement d'applications tierces, comme SpamAssassin ou OTRS.

Une personne malveillante pourrait construire un paquet de réponse DNS particulier, afin de perturber le système distant vulnérable.

5 Solution

Se référer à la mise à jour 0.63 de la bibliothèque Perl (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Debian DSA 1515 du 11 mars 2008 :
<http://www.debian.org/security/2008/dsa-1515>
- Référence CVE CVE-2007-6341 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6341>
- Note de mise à jour 0.63 de la bibliothèque Perl Net::DNS du 08 février 2008 :
<http://search.cpan.org/src/OLAF/Net-DNS-0.63/Changes>
- Rapport de bogue CPAN numéro 30316 :
<https://rt.cpan.org/Public/Bug/Display.html?id=30316>

Gestion détaillée du document

19 mars 2008 version initiale.