Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 09 septembre 2013
N° CERTA-2013-AVI-506

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans DNS Response Rate Limiting

Gestion du document

Référence	CERTA-2013-AVI-506
Titre	Vulnérabilité dans DNS Response Rate Limiting
Date de la première version	09 septembre 2013
Date de la dernière version	–
Source(s)	–
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(s)

– atteinte à l'intégrité des données

2 Systèmes affectés

– Bind versions 9.8 et 9.9
– NSD version 3.2.15
– Knot versions inférieures à 1.3.0

3 Résumé

Une vulnérabilité a été découverte dans *DNS Response Rate Limiting*. Elle permet à un attaquant de provoquer une atteinte à l'intégrité des données. RRL est une technologie de protection contre les attaques de type Déni de Services Distribués (DDoS) réalisées au travers de serveurs DNS faisant autorité sur leurs domaines. Lorsqu'elle est activée, le serveur DNS filtre certaines des réponses qu'il aurait du légitimement émettre. L'objectif de ce filtrage est d'atténuer les effets d'une attaque en cours. Le mécanisme appelé "slipping" en contrôle la fréquence et est un paramètre fondamental dont le choix de la valeur est l'objet de cet avis.

4 Contournement provisoire

Dans les solutions DNS affectées qui implémentent la technologie RRL, la valeur du paramètre "slip" configurée par défaut est égale à "2". Cette valeur introduit un risque d'attaques par pollution de cache DNS. Le CERTA recommande donc de positionner la valeur de ce paramètre à "1" qui annule ce risque.
Les modifications de configuration ci-dessous doivent être réalisées :

- Pour le logiciel "Bind", la version du patch RRL pour Bind antérieure au 4 avril 2013 est défaillante lorsque "slip" est positionné à la valeur "1". Une version ultérieure à cette date doit être utilisée pour corriger la vulnérabilité.
- Pour la version 3.2.15 de NSD, la valeur par défaut de slipping est "2", et cette dernière ne peut être reconfigurée. Il est recommandée d'utiliser les versions ultérieures.

5 Documentation

- Référence CVE CVE-2013-5661
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-5661

Gestion détaillée du document

09 septembre 2013 version initiale.