

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Mauvaise gestion du cache dans BIND 8

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-2003-AVI-205>

Gestion du document

Référence	CERTA-2003-AVI-205-002
Titre	Mauvaise gestion du cache dans BIND 8
Date de la première version	02 décembre 2003
Date de la dernière version	21 janvier 2004
Source(s)	Internet Software Consortium
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

Tout système fournissant un service DNS à l'aide de BIND 8, hormis les versions 8.3.7 et 8.4.3.

3 Résumé

Il est possible, pour l'administrateur mal intentionné d'un serveur DNS, de transmettre des réponses négatives qui seront stockées dans le cache des serveurs BIND 8 l'interrogeant, concernant des ressources pour lesquelles il n'est pourtant pas autorisé ("negative cache poisoning").

4 Description

Le principe du cache DNS consiste à stocker localement des données déjà reçues pour les restituer aux clients, avec un certain temps d'expiration, de manière à limiter la charge sur les serveurs autorisés des domaines cachés.

Un cache peut être pollué lorsqu’il garde des informations sur des ressources sans vérifier la légitimité du serveur, lui ayant transmis, pour ces données particulières. Il ne semble plus possible de polluer le cache d’un serveur BIND à jour avec des enregistrements usurpés, mais la présente faille permet de faire mémoriser au cache une information de “non-existence” d’une ressource. Les clients interrogeant le cache ne peuvent alors plus accéder à cette dernière.

5 Solution

Mettre à jour BIND 8 :

- Sources :
<http://www.isc.org/products/BIND/bind8.html>
- SuSE Linux :
http://www.suse.com/de/security/2003_47_bind8.html
- Sun Solaris :
<http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fslaert/57434>
- HP-UX :
<http://www4.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBUX0311-303>
- IBM AIX :
<http://www-1.ibm.com/support/docview.wss?uid=isg1IY49881>
<http://www-1.ibm.com/services/continuity/recover1.nsf/mss/MSS-OAR-E01-2003.1565.1>
- FreeBSD :
<ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-03:19.bind.asc>
- Debian :
<http://www.debian.org/security/2004/dsa-409>

6 Documentation

- Note de vulnérabilité du CERT/CC :
<http://www.kb.cert.org/vuls/id/734644>
- Référence CVE CAN-2003-0914 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0914>

Gestion détaillée du document

02 décembre 2003 version initiale ;

07 janvier 2004 ajout référence à l’avis de sécurité de Debian ;

20 janvier 2004 mise à jour IBM ;

21 janvier 2004 conflit dans les révisions du document : lien Debian restauré.