Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 07 août 2009
N° CERTA-2009-AVI-302-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans ISC BIND

Gestion du document

Référence	CERTA-2009-AVI-302-002
Titre	Vulnérabilité dans ISC BIND
Date de la première version	29 juillet 2009
Date de la dernière version	07 août 2009
Source(s)	Note d'information de l'ISC du 28 juillet 2009
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

ISC BIND 9 pour les versions antérieures à 9.4.3-P3, 9.5.1-P3 et 9.6.1-P1.

3 Résumé

Une vulnérabilité a été identifiée dans le service de gestion de noms de domaine ISC BIND. Cette dernière peut être exploitée par une personne malveillante, via des trames spécialement construites, afin de perturber le fonctionnement du service.

4 Description

Une vulnérabilité a été identifiée dans le service de gestion de noms de domaine ISC BIND. Ce dernier ne gère pas correctement les trames de mise à jour automatique concernant des zones sur lesquelles il a autorité et dont un enregistrement est de type `"ANY"`. La fonction vulnérable est `dns_db_findrdataset()`.

La vulnérabilité peut ainsi être exploitée par une personne malveillante, à distance via des trames spécialement construites, afin de perturber le fonctionnement du service.

La vulnérabilité fonctionne également si les mises à jour automatiques ne sont pas activées.

5 Solution

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

6 Documentation

- Avis de l'ISC, « Bind Dynamic Update DoS », 29 juillet 2009 :
  http://www.isc.org/node/474
- Mises à jour disponibles :
  ftp://ftp.isc.org/isc/bind9/9.4.3-P3/bind-9.4.3-P3.tar.gz
  ftp://ftp.isc.org/isc/bind9/9.5.1-P3/bind-9.5.1-P3.tar.gz
  ftp://ftp.isc.org/isc/bind9/9.6.1-P1/bind-9.6.1-P1.tar.gz
- Bulletin de sécurité Debian DSA-1847 :
  http://www.debian.org/security/2009/dsa-1847
- Bulletin de sécurité Ubuntu USN-808-1 :
  http://www.ubuntu.com/usn/usn-808-1
- Bulletins de sécurité RedHat RHSA-2009-1179, RHSA-2009-1180 et RHSA-2009-1181 :
  http://rhn.redhat.com/errata/RHSA-2009-1179.html
  http://rhn.redhat.com/errata/RHSA-2009-1180.html
  http://rhn.redhat.com/errata/RHSA-2009-1181.html
- Bulletins de sécurité OpenBSD :
  http://www.openbsd.org/errata44.html#014_bind
  http://www.openbsd.org/errata45.html#007_bind
  http://www.openbsd.org/errata46.html#001_bind
- Bulletin de sécurité FreeBSD :
  http://www.freebsd.org/advisories/FreeBSD-SA-09:12.bind.asc
- Bulletin de sécurité IBM AIX du 5 août 2009:
  http://aix.software.ibm.com/aix/efixes/security/bind_advisory.asc
- Référence CVE CVE-2009-0696 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0696

Gestion détaillée du document

29 juillet 2009 version initiale ;
30 juillet 2009 ajout des bulletins de sécurité Debian, Ubuntu, RedHat, OpenBSD, FreeBSD ;
07 août 2009 ajout du bulletin de sécurité IBM AIX.