Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 25 juillet 2008
N° CERTA-2008-AVI-359-003

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans ISC BIND

Gestion du document

Référence	CERTA-2008-AVI-359-003
Titre	Vulnérabilités dans ISC BIND
Date de la première version	09 juillet 2008
Date de la dernière version	25 juillet 2008
Source(s)	Annonce de mise à jour ISC BIND du 08 juillet 2008
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

Contournement de la politique de sécurité.

2 Systèmes affectés

- les versions d'ISC BIND antérieures à 9.5.0-P1 ;
- les versions d'ISC BIND antérieures à 9.4.2-P1 ;
- les versions d'ISC BIND antérieures à 9.3.5-P1.

La branche 8.x d'ISC BIND n'est plus maintenue depuis la fin du mois d'août 2007 et la dernière version disponible 8.4.7-P1 n'est donc pas corrigée.

3 Résumé

Des vulnérabilités ont été identifiées dans le serveur DNS ISC BIND. Elles permettraient à des personnes malveillantes de corrompre, sous certaines conditions, le cache et ainsi de rediriger du trafic vers des machines illégitimes.

4 Description

Des vulnérabilités ont été identifiées dans le serveur DNS ISC BIND. En particulier, le serveur ISC BIND utilise une plage de ports source trop restreinte pour émettre des requêtes DNS. Le serveur ne change également pas assez fréquemment ces valeurs de ports source. Ceci peut être exploité sous certaines conditions par une personne malveillante afin de corrompre le cache et rediriger du trafic vers des machines illégitimes.

5 Solution

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

6 Documentation

- Site officiel de l'ISC BIND :
  http://www.isc.org/sw/bind/
- Notes de mise à jour pour la version 9.5.0-P1 :
  http://www.isc.org/sw/bind/view/?release=9.5.0-P1#RELEASE
- Notes de mise à jour pour la version 9.4.2-P1 :
  http://www.isc.org/sw/bind/view/?release=9.4.2-P1#RELEASE
- Notes de mise à jour pour la version 9.3.5-P1 :
  http://www.isc.org/sw/bind/view/?release=9.3.5-P1#RELEASE
- Bulletin de sécurité Debian DSA-1603-1 du 08 juillet 2008 :
  http://list.debian.org/debian-security-announce/2008/msg00184.html
- Bulletin de sécurité Debian DSA-1604-1 du 08 juillet 2008 :
  http://list.debian.org/debian-security-announce/2008/msg00185.html
- Bulletin de sécurité Sun Solaris #239392 du 08 juillet 2008 :
  http://sunsolve.sun.com/search/document.do?assetkey=1-26-239392-1
- Bulletin de sécurité Red Hat RSA-2008:0533-3 du 08 juillet 2008 :
  http://rhn.redhat.com/errata/RHSA-2008-0533.html
- Bulletin de sécurité FreeBSD FreeBSD-SA-08:06.bind du 13 juillet 2008 :
  http://security.freebsd.org/advisories/FreeBSD-SA-08:06.bind
- Liste des mises à jour OpenBSD 4.2 :
  http://www.openbsd.org/errata42.html
- Liste des mises à jour OpenBSD 4.3 :
  http://www.openbsd.org/errata43.html
- Bulletin de sécurité HP-UX HPSBUX02351 SSRT080058 du 17 juillet 2008 :
  http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01506861
- Référence CVE CVE-2008-1447 :
  http://cve/mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1447

Gestion détaillée du document

09 juillet 2008 version initiale.
09 juillet 2008 ajout des références au CVE et aux bulletins de sécurité Debian, Red Hat et Sun.
16 juillet 2008 ajout de la référence au bulletin de sécurité FreeBSD.
25 juillet 2008 ajout des références aux correctifs pour OpenBSD et du bulletin de sécurité HP-UX.