



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 22 août 2007
N° CERTA-2007-AVI-327-005

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans BIND

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-2007-AVI-327>

Gestion du document

Référence	CERTA-2007-AVI-327-005
Titre	Vulnérabilité dans BIND
Date de la première version	24 juillet 2007
Date de la dernière version	22 août 2007
Source(s)	Bulletin de sécurité d'ISC BIND du 24 juillet 2007
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

- BIND 9.0 (toutes versions) ;
- BIND 9.1 (toutes versions) ;
- BIND 9.2.0, 9.2.1, 9.2.2, 9.2.3, 9.2.4, 9.2.5, 9.2.6, 9.2.7, 9.2.8 ;
- BIND 9.3.0, 9.3.1, 9.3.2, 9.3.3, 9.3.4 ;
- BIND 9.4.0, 9.4.1 ;
- BIND 9.5.0a1, 9.5.0a2, 9.5.0a3, 9.5.0a4, 9.5.0a5.

3 Résumé

Une vulnérabilité découverte dans BIND permet à une personne malintentionnée de contourner la politique de sécurité.

4 Description

Une vulnérabilité a été identifiée dans BIND. La faille concerne le générateur d'identifiants de requêtes, vulnérable à une cryptanalyse permettant une chance élevée de deviner le prochain identifiant pour la moitié des requêtes. Ceci peut être exploité par une personne malintentionnée pour effectuer du `cache poisoning` et donc contourner la politique de sécurité.

Une seconde vulnérabilité concerne les listes de contrôle d'accès (ACL) par défaut dans BIND. Elles ne prennent pas en compte la possibilité de faire des requêtes récursives ou d'interroger le cache.

5 Solution

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

6 Documentation

- Bulletin de sécurité ISC BIND du 24 juillet 2007 :
<http://www.isc.org/index.pl?sw/bind/bind-security.php>
- Bulletin de sécurité Gentoo GLSA-200708-13 du 18 août 2007 :
<http://www.gentoo.org/security/en/glsa/glsa-200708-13.xml>
- Bulletin de sécurité Mandriva MDKSA-2007:149 du 30 juin 2007 :
<http://www.mandriva.com/security/advisories?name=MDKSA-2007:149>
- Bulletin de sécurité Red Hat RHSA-2007-0740-2 du 24 juillet 2007 :
<http://rhn.redhat.com/errata/RHSA-2007-0740.html>
- Bulletin de sécurité Debian DSA 1341-1 du 25 juillet 2007 :
<http://lists.debian.org/debian-security-announce/debian-security-announce-2007/msg00102.html>
- Bulletin de sécurité Debian DSA 1341-2 du 26 juillet 2007 :
<http://lists.debian.org/debian-security-announce/debian-security-announce-2007/msg00103.html>
- Bulletin de sécurité Ubuntu USN-491-1 du 25 juillet 2007 :
<http://www.ubuntu.com/usn/usn-491-1>
- Bulletin de sécurité SuSE SUSE-SA:2007:047 du 01 août 2007 :
http://www.novell.com/linux/security/advisories/2007_47_bind.html
- Bulletin de sécurité FreeBSD FreeBSD-SA-07:07.bind du 01 août 2007 :
<http://security.freebsd.org/advisories/FreeBSD-SA-07:07.bind.asc>
- Référence CVE CVE-2007-2925 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2925>
- Référence CVE CVE-2007-2926 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2926>
- Référence CVE CVE-2007-3377 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3377>
- Page des mises à jour Nortel :
<http://support.nortel.com/go/main.jsp?cscat=BLTNDETAIL&id=623903#PRODUCTS>
- Réponse de Nortel à la vulnérabilité ISC:DNS:BIND 9, du 16 août 2007 :
<http://www116.nortel.com/pub/repository/CLARIFY/DOCUMENT/2007/33/022649-01.pdf>
- Bulletin de sécurité Avaya ASA-2007-351 du 15 août 2007 :
<http://support.avaya.com/elmodocs2/security/ASA-2007-351.htm>

Gestion détaillée du document

24 juillet 2007 version initiale.

26 juillet 2007 ajout des références aux bulletins de sécurité Debian, Ubuntu, Mandriva et Red Hat.

01 août 2007 ajout de la référence au bulletin de sécurité Debian.

02 août 2007 ajout des références aux bulletins de sécurité SuSE et FreeBSD.

17 août 2007 ajout des références aux CVE et aux bulletin de Nortel et Avaya.

22 août 2007 ajout de la référence au bulletin de sécurité Gentoo.