



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 31 janvier 2012
N° CERTA-2011-AVI-381-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités 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-2011-AVI-381>

Gestion du document

Référence	CERTA-2011-AVI-381-001
Titre	Multiples vulnérabilités dans Bind
Date de la première version	06 juillet 2011
Date de la dernière version	31 janvier 2012
Source(s)	Bulletins de sécurité ISC Bind du 05 juillet 2011
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

- les versions 9.6.3, 9.6-ESV-R4, 9.6-ESV-R4-P1, 9.6-ESV-R5b1 9.7.0, 9.7.0-P1, 9.7.0-P2, 9.7.1, 9.7.1-P1, 9.7.1-P2, 9.7.2, 9.7.2-P1, 9.7.2-P2, 9.7.2-P3, 9.7.3, 9.7.3-P1, 9.7.3-P2, 9.7.4b1 9.8.0, 9.8.0-P1, 9.8.0-P2, 9.8.0-P3 et 9.8.1b1 sont affectées par la vulnérabilité CVE-2011-2464 ;
- les versions 9.8.0, 9.8.0-P1, 9.8.0-P2 and 9.8.1b1 sont affectées par la vulnérabilité CVE-2011-2465.

3 Résumé

Deux vulnérabilités présentes dans Bind permettent à un utilisateur distant malintentionné de provoquer un déni de service.

4 Description

Deux vulnérabilités sont présentes dans le serveur DNS Bind :

- la première, de nature non-précisée par l'éditeur, permet à un utilisateur distant de provoquer un arrêt inopiné du service `named` par le biais d'un paquet construit de façon particulière.
- la seconde concerne la mise en œuvre des `Response Policy Zone (RPZ)` et permet, sous certaines conditions, à un utilisateur distant de provoquer un déni de service.

5 Solution

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

6 Documentation

- Bulletins de sécurité ISC Bind du 05 juillet 2011 :
<http://www.isc.org/software/bind/advisories/cve-2011-2464>
<http://www.isc.org/software/bind/advisories/cve-2011-2465>
- Bulletin de sécurité Debian DSA 2272 du 05 juillet 2011 :
<http://www.debian.org/security/2011/dsa-2272>
- Bulletin de sécurité Ubuntu USN-1163-1 du 05 juillet 2011 :
<http://www.ubuntu.com/usn/usn-1163-1>
- Bulletin de sécurité HP du 20 janvier 2012 :
<http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c03070783>
- Référence CVE CVE-2011-2464 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2464>
- Référence CVE CVE-2011-2465 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2465>

Gestion détaillée du document

06 juillet 2011 version initiale.

31 janvier 2012 ajout du bulletin de sécurité HP.