

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans la bibliothèque libspf2

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-2008-AVI-526>

Gestion du document

Référence	CERTA-2008-AVI-526
Titre	Vulnérabilité dans la bibliothèque libspf2
Date de la première version	24 octobre 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité Debian DSA-1659 du 23 octobre 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

- Exécution de code arbitraire à distance ;
- déni de service à distance.

2 Systèmes affectés

- libspf2 versions 1.x.

3 Résumé

Une vulnérabilité dans la bibliothèque libspf2 permet à un utilisateur malintentionné de provoquer un déni de service ou d'exécuter du code arbitraire à distance.

4 Description

Une vulnérabilité de type débordement de mémoire a été découverte dans la fonction `SPF_dns_resolv_lookup()` présente dans le fichier source `Spf_dns_resolv.c`. Cette vulnérabilité peut être exploitée au moyen d'une réponse DNS (*Domain Name System*) spécialement construite pour provoquer un déni de service ou exécuter du code arbitraire à distance.

5 Solution

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

6 Documentation

- Bulletin de sécurité Debian DSA-1659 du 23 octobre 2008 :
<http://www.debian.org/security/2008/dsa-1659>
- Référence CVE CVE-2008-2469 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2469>

Gestion détaillée du document

24 octobre 2008 version initiale.