

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans libxslt

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-282>

Gestion du document

Référence	CERTA-2008-AVI-282
Titre	Vulnérabilité dans libxslt
Date de la première version	29 mai 2008
Date de la dernière version	-
Source(s)	Bulletin de sécurité RedHat RHSA-2008-0287 du 21 mai 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

- Déni de service à distance ;
- exécution de code arbitraire à distance.

2 Systèmes affectés

libxslt versions 1.x.

3 Résumé

Une vulnérabilité présente dans la bibliothèque de fonctions `libxslt` permet à un utilisateur distant de provoquer un déni de service de la machine vulnérable ou d'exécuter du code arbitraire.

4 Description

Une vulnérabilité a été identifiée dans la bibliothèque de fonctions `libxslt`. Celle-ci est relative à la mise en œuvre des feuilles de styles XSL. Elle permet à un utilisateur distant malintentionné de provoquer un déni de service ou d'exécuter du code arbitraire via un fichier au format XSL construit de façon particulière.

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 1589 du 29 mai 2008 :
<http://www.debian.org/security/dsa-1589>
- Bulletin de sécurité RedHat RHSA-2008:0287 du 21 mai 2008 :
<http://rhn.redhat.com/errata/RHSA-2008-0287.html>
- Référence CVE CVE-2008-1767 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1767>

Gestion détaillée du document

29 mai 2008 version initiale.