

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de 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-387>

Gestion du document

Référence	CERTA-2008-AVI-387
Titre	Vulnérabilité de libxslt
Date de la première version	01 août 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité Debian DSA-1624
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

libxslt versions 1.1.24 et antérieures.

3 Résumé

Une vulnérabilité présente dans `libxslt` permet à un utilisateur distant de provoquer un déni de service ou potentiellement d'exécuter du code arbitraire.

4 Description

Une erreur est présente dans la bibliothèque de fonctions `libxslt`. La vulnérabilité est relative aux fonctions utilisées pour mettre en œuvre du chiffrement de type RC4 au sein d'un fichier XSLT. Un utilisateur distant malintentionné pourra ainsi provoquer un déni de service ou exécuter du code arbitraire au moyen d'une feuille de style XSLT construite de façon particulière.

5 Solution

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

6 Documentation

- Bulletin de sécurité Debian DSA 1624 du 31 juillet 2008 :
<http://www.debian.org/security/dsa-1624>
- Bulletin de sécurité RedHat RHSA-2008:0649 du 31 juillet 2008 :
<http://rhn.redhat.com/errata/RHSA-2008-0649.html>
- Référence CVE CVE-2008-2935 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2935>

Gestion détaillée du document

01 août 2008 version initiale.