

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de la bibliothèque libxml2

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-2004-AVI-051>

Gestion du document

Référence	CERTA-2004-AVI-051-004
Titre	Vulnérabilité de la bibliothèque libxml2
Date de la première version	27 février 2004
Date de la dernière version	12 mai 2004
Source(s)	Avis de sécurité RedHat RHSA-2004:090-06
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.

2 Systèmes affectés

Bibliothèque libxml2 version 2.6.5 et antérieures.

3 Résumé

Une vulnérabilité de type débordement de mémoire a été découverte dans la bibliothèque libxml2.

4 Description

La bibliothèque libxml2 sert pour le traitement des données au format XML. Elle est notamment utilisée par les bureaux *Gnome* et *KDE* sur les plates-formes Unix.

Lorsque la bibliothèque libxml2 analyse des données depuis une ressource distante via FTP ou HTTP, elle utilise des routines spécifiques pour traiter les données.

Si une URL très longue est utilisée, il est possible de provoquer un débordement de mémoire. Cette vulnérabilité peut être exploitée par un utilisateur distant mal intentionné pour exécuter du code arbitraire sur le système vulnérable.

5 Solution

Appliquer le correctif de l'éditeur.

6 Documentation

- Avis de sécurité RedHat RHSA-2004:090-06 :
<http://rhn.redhat.com/errata/RHSA-2004-090.html>
- Avis de sécurité RedHat RHSA-2004:091-07 :
<http://rhn.redhat.com/errata/RHSA-2004-091.html>
- Avis de sécurité Debian DSA 455-1 :
<http://www.debian.org/security/2004/dsa-455>
- Avis de sécurité Mandrake MDKSA-2004:018 :
<http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2004:018>
- Avis de sécurité Gentoo GLSA 200403-01 :
<http://lists.netsys.com/pipermail/full-disclosure/2004-March/018344.html>
- Avis de sécurité FreeBSD du 25 février 2004 :
<http://www.vuxml.org/freebsd/>
- Mise à jour de sécurité du paquetage NetBSD libxml2 :
<ftp://ftp.netbsd.org/pub/NetBSD/packages/distfiles/vulnerabilities>
- Référence CVE CAN-2004-0110 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0110>

Gestion détaillée du document

27 février 2004 version initiale.

03 mars 2004 corrections et mises à jour des références aux bulletins de sécurité RedHat.

04 mars 2004 ajout des références aux bulletins de sécurité Debian et Mandrake.

08 mars 2004 ajout de la référence au bulletin de sécurité Gentoo.

12 mai 2004 ajout références aux bulletins de sécurité FreeBSD et NetBSD.