Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 20 décembre 2004
N° CERTA-2004-AVI-361-004

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités de libxml2

Gestion du document

Référence	CERTA-2004-AVI-361-004
Titre	Multiples vulnérabilités de libxml2
Date de la première version	04 novembre 2004
Date de la dernière version	20 décembre 2004
Source(s)	Bulletin de sécurité GLSA 200411-05 de Gentoo
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.

2 Systèmes affectés

libxml2 versions 2.6.14 et antérieures.

3 Description

La bibliothèque libxml2 sert pour le traitement des données au format XML. Elle est notamment utilisée par l'environnement graphique Gnome.

Deux vulnérabilités de type débordement de mémoire sont présentes dans des routines utilisées pour le traitement de liens (URI) dans le module `nanoftp`. Plusieurs vulnérabilités de type débordement de mémoire sont également présentes dans des routines utilisées pour la résolution de noms dans les modules `nanoftp` et `nanohttp`.

Au moyen d'un fichier XML habilement constitué, les vulnérabilités affectant le traitement de liens (URI) peuvent être exploitées par un utilisateur mal intentionné afin d'exécuter du code arbitraire via une application utilisant la bibliothèque vulnérable.

Les vulnérabilités relatives à la résolution de noms peuvent être exploitées au travers d'un serveur DNS hostile contrôlé par un utilisateur mal intentionné.

4 Solution

La version 2.6.15 de la bibliothèque `libxml2` corrige cette vulnérabilité.
Se référer aux bulletins de sécurité de l'éditeur (cf. section Documentation) pour l'obtention des correctifs.

5 Documentation

- Sortie de la version 2.6.15 de libxml2 :
  http://www.xmlsoft.org/news.html
- Bulletin de sécurité Debian DSA-582 du 02 novembre 2004 :
  http://www.debian.org/security/2004/dsa-582
- Bulletin de sécurité Gentoo GLSA 200411-05 du 02 novembre 2004 :
  http://www.gentoo.org/security/en/glsa/glsa-200411-05.xml
- Bulletin de sécurité Mandrake MDKSA-2004:127 :
  http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:127
- Bulletin de sécurité Red Hat RHSA-2004:615 du 12 novembre 2004 :
  http://rhn.redhat.com/errata/RHSA-2004-615.html
- Bulletin de sécurité Red Hat RHSA-2004:650 du 16 décembre 2004 :
  http://rhn.redhat.com/errata/RHSA-2004-650.html
- Mise à jour de sécurité des paquetages NetBSD libxml et libxml2 :
  ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/textproc/libxml/README.html
  ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/textproc/libxml2/README.html
- Référence CVE CAN-2004-0989 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0989

Gestion détaillée du document

04 novembre 2004 version initiale.
05 novembre 2004 ajout du bulletin de sécurité Mandrake.
16 novembre 2004 ajout de la référence au bulletin de sécurité RHSA-2004:615 de Red Hat.
22 novembre 2004 ajout des références aux bulletins de sécurité NetBSD pour libxml et libxml2.
20 décembre 2004 ajout de la référence au bulletin de sécurité Red Hat (RHSA-2004:650) relatif à libxml.