Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 18 avril 2011
N° CERTA-2011-AVI-231

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans kde4libs

Gestion du document

Référence	CERTA-2011-AVI-231
Titre	Vulnérabilités dans kde4libs
Date de la première version	18 avril 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité Ubuntu USN-1110-1
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

- Injection de code indirecte à distance ;
- *man-in-the-middle*.

2 Systèmes affectés

- Ubuntu 10.10 ;
- Ubuntu 10.04 LTS ;
- Ubuntu 9.10.

3 Résumé

Plusieurs vulnérabilités permettant une injection de code indirecte à distance ainsi qu'une attaque de type *man-in-the-middle* ont été découvertes dans *kde4libs*.

4 Description

Deux vulnérabilités ont été découvertes dans *kde4libs*.

La première (CVE-2011-1094) permet à une personne malintentionnée d'effectuer une attaque de type *man-in-the-middle*. Cette faille provient d'une mauvaise gestion des certificats `SSL` par le module *KDE KSSL*, lorsque que ces derniers ont été émis pour une adresse *IP*.

La seconde (CVE-2011-1168) permet d'injecter indirectement du code à distance. Le module *KDE KHTML* ne protège pas correctement les `urls` lors de la génération de pages d'erreur, autorisant ainsi un attaquant à injecter indirectement du code via une *url* spécialement conçue.

5 Solution

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

6 Documentation

- Bulletin de sécurité Ubuntu USN-1110-1 du 14 avril 2011 :
  http://www.ubuntulinux.org/usn/usn-1110-1
- Référence CVE CVE-2011-1094 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1094
- Référence CVE CVE-2011-1168 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1168

Gestion détaillée du document

18 avril 2011 version initiale.