Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 21 décembre 2004
N° CERTA-2004-AVI-206-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Aspell

Gestion du document

Référence	CERTA-2004-AVI-206-002
Titre	Vulnérabilité de Aspell
Date de la première version	23 juin 2004
Date de la dernière version	21 décembre 2004
Source(s)	Avis de sécurité Nettwerked UK du 08 juin 2004
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 ;
- exécution de code arbitraire à distance.

2 Systèmes affectés

Toutes les versions de Aspell.

3 Résumé

Une vulnérabilité dans la manipulation des dictionnaires par Aspell permet à un utilisateur mal intentionné de réaliser un déni de service ou d'exécuter du code arbitraire sur la machine vulnérable.

4 Description

Aspell est un logiciel de correction orthographique.
Aspell contient un utilitaire de compression et décompression de listes de mots appelé `word-list-compress`. Une vulnérabilité dans cet utilitaire permet à un utilisateur mal intentionné, via un dictionnaire habilement constitué, de réaliser un déni de service ou d'exécuter du code arbitraire.

5 Solution

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

6 Documentation

- Site Internet de Aspell :
  http://aspell.sourceforge.net
- Bulletin de sécurité de Nettwerked UK du 08 juin 2004 :
  http://nettwerked.mg2.org/advisories/wlc
- Bulletin de sécurité OpenBSD pour Aspell du 19 juin 2004 :
  http://www.vuxml.org/openbsd/
- Bulletin de sécurité Gentoo GLSA 200406-14 du 17 juin 2004 :
  http://www.gentoo.org/security/en/glsa/glsa-200406-14.xml
- Bulletin de sécurité Mandrake MDKSA-2004:153 du 21 décembre 2004 :
  http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:153
- Référence CVE CAN-2004-0548 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0548

Gestion détaillée du document

23 juin 2004 version initiale.
24 juin 2004 ajout référence au bulletin de sécurité de Gentoo.
21 décembre 2004 ajout référence au bulletin de sécurité de Mandrake. Ajout référence CVE.