



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 30 juillet 2004
N° CERTA-2004-AVI-243-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de la bibliothèque wv

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-243>

Gestion du document

Référence	CERTA-2004-AVI-243-001
Titre	Vulnérabilité de la bibliothèque wv
Date de la première version	15 juillet 2004
Date de la dernière version	30 juillet 2004
Source(s)	Bulletin de sécurité Gentoo GLSA 200407-11
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

wv versions 0.7.4, 0.7.5, 0.7.6 et 1.0.0.

3 Résumé

Une vulnérabilité dans la bibliothèque wv permet à un utilisateur mal intentionné d'exécuter du code arbitraire sur la plate-forme vulnérable.

4 Description

La bibliothèque wv permet la lecture des documents au format Microsoft Word sous les environnements UNIX. Une vulnérabilité de type débordement de tampon permet à un utilisateur mal intentionné, via un fichier malicieusement construit et destiné à être lu par wv, d'exécuter du code arbitraire sur la plate-forme vulnérable. Ceci n'est possible que dans le mode HTML view.

5 Contournement provisoire

- Ne pas lire de fichiers non surs avec `wvHtml` ou des applications utilisant la bibliothèque `wv` ;
- Lors de la lecture d'un fichier non sur avec `wvHtml` ou une application utilisant la bibliothèque `wv`, s'assurer que le mode `HTML view` est désactivé.

6 Solution

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

7 Documentation

- Site Internet de la bibliothèque `wv` (projet `wvWare`) :
<http://wwwware.sourceforge.net>
- Bulletin de sécurité iDEFENSE du 09 juillet 2004 :
<http://www.odefense.com/application/poi/display?id=115&type=vulnerabilities>
- Bulletin de sécurité Gentoo GLSA 200407-11 du 14 juillet 2004 :
<http://www.gentoo.org/security/en/glsa/glsa-200407-11.xml>
- Bulletin de sécurité Mandrake MDKSA-2004:077 du 29 juillet 2004 :
<http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:077>
- Référence CVE CAN-2004-0645 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0645>

Gestion détaillée du document

15 juillet 2004 version initiale.

30 juillet 2004 ajout de la référence au bulletin de sécurité Mandrake.