Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 25 janvier 2005
N° CERTA-2004-AVI-373-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de unarj

Gestion du document

Référence	CERTA-2004-AVI-373-002
Titre	Vulnérabilité de unarj
Date de la première version	22 novembre 2004
Date de la dernière version	25 janvier 2005
Source(s)	Bulletin de sécurité Gentoo GLSA 200411-29 du 19 novembre 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

Exécution de code arbitraire à distance.

2 Systèmes affectés

- `unarj` pour Gentoo version 2.63a-r1 et versions antérieures ;
- `unarj` pour FreeBSD version 2.43_1 et versions antérieures ;
- `unarj` pour Debian en version antérieure à 2.43-3woody1.

3 Résumé

Deux vulnérabilités dans `unarj` permettent à un utilisateur mal intentionné d'exécuter du code arbitraire à distance.

4 Description

`unarj` est un outil de décompression d'archives au format ARJ.
Deux vulnérabilités sont présentes dans `unarj` : une vulnérabilité de type débordement de mémoire et une vulnérabilité de type traversée de répertoire.

Ces vulnérabilités peuvent être exploitées par un utilisateur mal intentionné afin d'exécuter du code arbitraire sur la plate-forme vulnérable.

5 Solution

La version 2.63a-r2 de `unarj` pour Gentoo corrige cette vulnérabilité.
La version 2.43_2 de `unarj` pour FreeBSD corrige cette vulnérabilité.
Se référer au bulletin de sécurité de l'éditeur (cf. section Documentation) pour l'obtention des correctifs.

6 Documentation

- Site Internet de `unarj` :
  http://www.arjsoftware.com
- Bulletin de sécurité Gentoo GLSA 200411-29 du 19 novembre 2004 :
  http://www.gentoo.org/security/en/glsa/glsa-200411-29.xml
- Bulletin de sécurité FreeBSD pour unarj du 26 novembre 2004 :
  http://www.vuxml.org/freebsd/
- Bulletin de sécurité Debian du 21 janvier 2005 :
  http://www.debian.org/security/2005/dsa-652
- Référence CVE CAN-2004-0947 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0947
- Référence CVE CAN-2004-1027 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1027

Gestion détaillée du document

22 novembre 2004 version initiale.
29 novembre 2004 ajout de la référence au bulletin de sécurité FreeBSD.
25 janvier 2005 ajout de la référence au bulletin de sécurité Debian.