Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 23 juin 2005
N° CERTA-2005-AVI-085-003

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de unace

Gestion du document

Référence	CERTA-2005-AVI-085-003
Titre	Vulnérabilité de unace
Date de la première version	24 février 2005
Date de la dernière version	23 juin 2005
Source(s)	Bulletin de sécurité FreeBSD du 22 février 2005
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

- Contournement de la politique de sécurité ;
- déni de service ;
- exécution de code arbitraire.

2 Systèmes affectés

`unace` version 1.2b (dernière version libre) et versions antérieures.

3 Résumé

Plusieurs vulnérabilités dans `unace` permettent à un utilisateur mal intentionné de contourner la politique de sécurité (altérer des données), réaliser un déni de service ou exécuter du code arbitraire à distance sur la plate-forme vulnérable.

4 Description

`unace` est un outil de manipulation d'archives au format ACE.
Plusieurs vulnérabilités sont présentes dans `unace` :

- Des vulnérabilités de type débordement de mémoire dans la manipulation d'archives au format ACE malicieusement construites (CAN-2005-0160) ;
- des vulnérabilités de type traversée de répertoires (`directory traversal`) lors de l'extraction d'archives au format ACE malicieusement construites (CAN-2005-0161) ;
- des vulnérabilités de type débordement de mémoire dans la manipulation des arguments passés à l'exécutable `unace` particulièrement longs (CAN-2005-0160).

Ces vulnérabilités permettent à un utilisateur mal intentionné de contourner la politique de sécurité (altérer des données), réaliser un déni de service ou exécuter du code arbitraire à distance sur la plate-forme vulnérable.

5 Solution

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

6 Documentation

- Site Internet de `unace` :
  http://www.winace.com
- Bulletin de sécurité FreeBSD pour `unace` du 22 février 2005 :
  http://www.vuxml.org/freebsd/pkg-unace.html
- Bulletin de sécurité OpenBSD pour `unace` du 22 février 2005 :
  http://www.vuxml.org/openbsd/pkg-unace.html
- Bulletin de sécurité Gentoo GLSA 200502-32 du 28 février 2005 :
  http://www.gentoo.org/security/en/glsa/glsa-200502-32.html
- Mise à jour de sécurité du paquetage NetBSD unace :
  ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/archivers/unace/README.html
- Bulletin de sécurité SUSE SUSE-SR:2005:016 du 17 juin 2005 :
  http://www.novell.com/linux/security/advisories/2005_16_sr.html
- Référence CVE CAN-2005-0160 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0160
- Référence CVE CAN-2005-0161 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0161

Gestion détaillée du document

24 février 2005 version initiale.
01 mars 2005 ajout de la référence au bulletin de sécurité Gentoo.
03 mars 2005 ajout de la référence au bulletin de sécurité NetBSD.
23 juin 2005 ajout de la référence au bulletin de sécurité SUSE.