Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 08 décembre 2005
N° CERTA-2005-AVI-383-003

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans UW-imapd

Gestion du document

Référence	CERTA-2005-AVI-383-003
Titre	Vulnérabilité dans UW-imapd
Date de la première version	06 octobre 2005
Date de la dernière version	08 décembre 2005
Source(s)	Bulletin de sécurité iDEFENSE #313 du 04 octobre 2005
Pièce(s) jointe(s)	

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 ;
- déni de service.

2 Systèmes affectés

Toutes les versions de UW-imapd.

3 Résumé

Une vulnérabilité découverte dans l'application UW-imapd permet à un utilisateur distant mal intentionné de causer un déni de service ou d'exécuter du code arbitraire.

4 Description

UW-Imap est le serveur de messagerie IMAP (Internet Message Access Protocol) développé par l'université de Washington.

La vulnérabilité de type débordement de pile est causée par une erreur dans la fonction `mail_valid_net_parse_work()`. Cette vulnérabilité peut être exploitée par une personne malveillante au moyen d'une boîte mél malicieusement nommée.

5 Solution

La mise à jour de sécurité pour UW-imapd est disponible à l'adresse suivante :
ftp://ftp.cac.washington.edu/imap/

6 Documentation

- Bulletin de sécurité iDEFENSE #313 du 04 octobre 2005 :
  http://www.idefense.com/application/poi/display?id=313&type=vulnerabilities
- Bulletin de sécurité Gentoo GLSA 200510-10 du 11 octobre 2005 :
  http://security.gentoo.org/glsa/glsa-200510-10.xml
- Bulletin de sécurité Debian DSA-861 du 11 octobre 2005 :
  http://www.debian.org/security/2005/dsa-861
- Bulletin de sécurité RedHat RHSA-2005:850 du 06 décembre 2005 :
  http://rhn.redhat.com/errata/RHSA-2005-850.html
- Référence CVE CAN-2005-2933 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2933

Gestion détaillée du document

06 octobre 2005 version initiale.
11 octobre 2005 ajout de la référence au bulletin de sécurité Gentoo GLSA 200510-10.
12 octobre 2005 ajout de la référence au bulletin de sécurité Debian DSA-861.
08 décembre 2005 ajout de la référence au bulletin de sécurité RedHat RHSA-2005:850.