

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité du serveur wu-imapd

---

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-2002-AVI-115>

---

### Gestion du document

Référence	CERTA-2002-AVI-115
Titre	Vulnérabilité du serveur wu-imapd
Date de la première version	31 mai 2002
Date de la dernière version	–
Source(s)	Avis RedHat RHSA-2002:092-11 Avis Mandrake MDKSA-2002:034
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

Serveur wu-imapd développé par l'Université de Washington.

## 3 Résumé

Le serveur wu-imapd développé par l'Université de Washington est vulnérable à une attaque de type débordement de mémoire.

## 4 Description

IMAP (Internet Message Access Protocol) est un protocole de messagerie électronique. Une vulnérabilité de type débordement de mémoire présente dans le serveur wu-imapd permet à un utilisateur mal intentionné d'exécuter du code arbitraire avec ses privilèges (*UID* et *GID*).

Pour pouvoir exploiter cette vulnérabilité, l'attaquant doit au préalable s'authentifier auprès du serveur.

## **5 Solution**

Contactez votre éditeur pour la mise à jour de votre serveur.

## **6 Documentation**

- Avis RedHat RHSA-2002:092-11 :  
<http://rhn.redhat.com/errata/RHSA-2002-092.html>
- Avis Mandrake MDKSA-2002:034 :  
<http://www.linux-mandrake.com/en/security/>

## **Gestion détaillée du document**

**31 mai 2002** version initiale.