

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans Ipswitch Imail Server

---

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-045>

---

### Gestion du document

Référence	CERTA-2004-AVI-045
Titre	Vulnérabilité dans Ipswitch Imail Server
Date de la première version	20 février 2004
Date de la dernière version	–
Source(s)	Bulletin de sécurité 02.17.04 de iDEFENSE
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

IMail Server d'Ipswitch sous Windows.

## 3 Résumé

Une vulnérabilité présente dans le serveur de courrier IMail Server d'Ipswitch permet à un utilisateur distant mal intentionné d'exécuter du code arbitraire avec les privilèges de l'administrateur.

## 4 Description

IMail Server est un serveur de courrier utilisé sur les plateformes Windows.

Une vulnérabilité dans le démon LDAP d'IMail Server permet à un utilisateur distant, par le biais d'une requête judicieusement composée, d'exploiter un débordement de mémoire sur la machine cible et d'exécuter ainsi du code arbitraire avec les privilèges de l'administrateur.

## **5 Solution**

Télécharger le correctif disponible sur le site de l'éditeur :

[http://www.ipswitch.com/support/imap/releases/imap\\_professional/im805HF2.html](http://www.ipswitch.com/support/imap/releases/imap_professional/im805HF2.html)

## **6 Documentation**

Bulletin de sécurité 02.17.04 de iDEFENSE :

<http://www.odefense.com/application/poi/display?id=74>

## **Gestion détaillée du document**

**20 février 2004** version initiale.