

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans MDaemon

---

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-2008-AVI-146>

---

### Gestion du document

Référence	CERTA-2008-AVI-146
Titre	Vulnérabilité dans MDaemon
Date de la première version	19 mars 2008
Date de la dernière version	–
Source(s)	Notes de version de MDaemon 9.65 du 14 mars 2008
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

*MDaemon* versions 9.64 et antérieures.

## 3 Résumé

Une vulnérabilité dans le service IMAP de *MDaemon* permet à un utilisateur authentifié d'exécuter du code arbitraire à distance.

## 4 Description

Une vulnérabilité a été découverte dans le traitement des requêtes `fetch` par le service IMAP de *MDaemon*. L'exploitation de cette vulnérabilité permet l'exécution de code arbitraire à distance mais nécessite l'utilisation des identifiants d'un compte valide.

## **5 Solution**

Mettre à jour *MDaemon* en version 9.65 (cf. section Documentation).

## **6 Documentation**

- Notes de version de *MDaemon* 9.65 du 14 mars 2008 :  
[http://files.altn.com/MDaemon/Release/RelNotes\\_en.txt](http://files.altn.com/MDaemon/Release/RelNotes_en.txt)
- Téléchargement de *MDaemon* 9.65 :  
<http://www.altn.com/Downloads/ExistingCustomers/>

## **Gestion détaillée du document**

**19 mars 2008** version initiale.