

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans MAILsweeper de Clearswift

---

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-2006-AVI-253>

---

### Gestion du document

Référence	CERTA-2006-AVI-253
Titre	Multiples vulnérabilités dans MAILsweeper de Clearswift
Date de la première version	23 juin 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité mimesweeper du 21 juin 2006
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

- Dénis de service à distance ;
- contournement de la politique de sécurité.

## 2 Systèmes affectés

- Clearswift MAILsweeper 4.x pour Microsoft Exchange 2000 ;
- Clearswift MAILsweeper 4.x pour SMTP.

## 3 Résumé

Plusieurs vulnérabilités découvertes dans MAILsweeper permettent à un utilisateur mal intentionné de contourner la politique de sécurité ou de provoquer un déni de service à distance.

## 4 Description

L'application MAILsweeper de Clearswift analyse les courriers électroniques entrants.

- Une vulnérabilité dans la gestion de certains messages permet à une personne malveillante, au moyen d'un message électronique astucieusement formé de contourner la politique de sécurité du système et de passer outre la vérification du message ;
- une vulnérabilité dans le traitement des requêtes de résolution de nom inverse peut être exploitée par un utilisateur malveillant au moyen d'un message électronique astucieusement construit afin de provoquer un déni de service ;
- une erreur dans le traitement des messages électroniques malformées permet à un individu mal intentionné de provoquer forcer l'arrêt du service.

## **5 Solution**

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

## **6 Documentation**

- Site internet de l'éditeur :  
<http://www.clearswift.com/>
- Bulletin de sécurité mimesweeper du 21 juin 2006 :  
[http://download.mimesweeper.com/www/TechnicalDocumentation/ReadMe\\_MSW\\_4.3.20.htm](http://download.mimesweeper.com/www/TechnicalDocumentation/ReadMe_MSW_4.3.20.htm)

## **Gestion détaillée du document**

**23 juin 2006** version initiale.