

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans MailEnable

---

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-2005-AVI-510>

---

### Gestion du document

Référence	CERTA-2005-AVI-510
Titre	Multiples vulnérabilités dans MailEnable
Date de la première version	29 décembre 2005
Date de la dernière version	–
Source(s)	Forum de Discussion Full-Disclosure
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 ;
- déni de service à distance.

## 2 Systèmes affectés

- MailEnable Enterprise Edition 1.71 et versions antérieures ;
- MailEnable Professional 1.1 et versions antérieures.

## 3 Résumé

Plusieurs vulnérabilités dans l'application MailEnable permettent à un utilisateur mal intentionné de provoquer un déni de service ou d'exécuter du code arbitraire à distance.

## 4 Description

MailEnable est un serveur de messagerie.

Ces vulnérabilités sont dues à une erreur dans le traitement des arguments fournis aux commandes IMAP (Internet Message Access Protocol) suivantes : UID FETCH, LIST et LSUB. Un individu mal intentionné peut, au moyen d'arguments malicieusement constitués exécuter du code arbitraire à distance ou provoquer un déni de service.

## **5 Solution**

Appliquer la mise à jour de sécurité ME-10010 disponible à l'adresse suivante :  
<http://www.mailenable.com/hotfix/ME-10010.EXE>

## **6 Documentation**

- Information sur le Forum de discussion « Full-Disclosure »  
<http://lists.grok.org.uk/pipermail/full-disclosure/2005-December/040388.html>
- Mise à jour de sécurité ME-10010 :  
<http://www.mailenable.com/hotfix/ME-10010.EXE>

## **Gestion détaillée du document**

**29 décembre 2005** version initiale.