

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : 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-377>

Gestion du document

Référence	CERTA-2005-AVI-377
Titre	Vulnérabilités dans MailEnable
Date de la première version	04 octobre 2005
Date de la dernière version	–
Source(s)	
Pièce(s) jointe(s)	

TAB. 1 – Gestion du document

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

- Déni de service ;
- exécution de code arbitraire.

2 Systèmes affectés

- MailEnable Professional version 1.6 et antérieures ;
- MailEnable Enterprise version 1.1 et antérieures.

3 Description

MailEnable est un serveur de messagerie qui présente une vulnérabilité de type débordement de mémoire au niveau de la gestion des logs W3C. Cette vulnérabilité pourrait permettre à un attaquant de provoquer un déni de service ou encore d'exécuter du code arbitraire.

4 Documentation

- Site Internet de MailEnable :
<http://www.mailenable.com/hotfix>
- Bulletin de sécurité de Secunia :
<http://secunia.com/advisories/17010>

Gestion détaillée du document

04 octobre 2005 version initiale.