

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans `qmailadmin`

---

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-123>

---

## Gestion du document

Référence	CERTA-2006-AVI-123
Titre	Vulnérabilité dans <code>qmailadmin</code>
Date de la première version	22 mars 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité de Secunia
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

`qmailadmin` versions sources 1.2.8 et 1.2.9.

## 3 Résumé

Un utilisateur distant mal intentionné peut utiliser un lien réticulaire (URL) habilement construit pour exécuter du code arbitraire sur le système hôte du programme `qmailadmin` avec les droits de l'administrateur.

## 4 Description

`qmailadmin` est utilitaire de gestion par interface « web » des domaines virtuels d'un service de messagerie utilisant `qmail`. Ce programme est invoqué par un serveur « web » hôte.

Un débordement de tampon dans la gestion des informations sur la requête transmises par le serveur peut être utilisée pour exécuter du code arbitraire avec les privilèges du programme, soit `root`.

## **5 Contournement provisoire**

Restreindre à l'accès à l'interface « web » d'administration à des systèmes de confiance au moyen d'un pare-feu ou de directives dans la configuration du serveur.

## **6 Solution**

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation) ou mettre à jour les sources en version 1.2.10 au moins.

## **7 Documentation**

- Site internet de qmailadmin :  
<http://www.inter7.com/index.php?page=qmailadmin>
- Bulletin de sécurité Secunia #19262 du 17 mars 2006 :  
<http://secunia.com/advisories/19262/>
- Référence CVE CAN-2006-1141 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2006-1141>

## **Gestion détaillée du document**

**22 mars 2006** version initiale.