

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans le webmail de Kerio MailServer

---

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-2009-AVI-227>

---

### Gestion du document

Référence	CERTA-2009-AVI-227
Titre	Vulnérabilité dans le webmail de Kerio MailServer
Date de la première version	10 juin 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité Kerio KSEC-2009-06-08-01 du 08 juin 2009
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

Injection de code indirecte.

## 2 Systèmes affectés

- Kerio MailServer 6.6.2 et versions antérieures ;
- Kerio MailServer 6.7.0.

## 3 Résumé

Une vulnérabilité de type injection de code indirecte (*cross-site scripting*) a été identifiée dans Kerio MailServer.

## 4 Description

Une vulnérabilité de type injection de code indirecte a été identifiée dans le *webmail* de Kerio MailServer. Elle peut être exploitée par une personne malintentionnée pour accéder aux données personnelles d'une victime en l'incitant à cliquer sur un lien spécialement conçu.

## **5 Solution**

Le patch 3 de la version 6.6.2 et le patch 1 de la version 6.7.0 corrigent le problème.

## **6 Documentation**

- Bulletin de sécurité KSEC-2009-06-08-01 du 08 juin 2009 :  
<http://www.kerio.com/support/security-advisories#0906>
- Page de téléchargement de Kerio MailServer :  
<http://www.kerio.com/mailserver/download>

## **Gestion détaillée du document**

**10 juin 2009** version initiale.