



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité
des systèmes d'information
CERTA

Paris, le 20 février 2008
N° CERTA-2008-AVI-096

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans 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-2008-AVI-096>

Gestion du document

| | |
|-----------------------------|---|
| Référence | CERTA-2008-AVI-096 |
| Titre | Vulnérabilités dans Kerio MailServer |
| Date de la première version | 20 février 2008 |
| Date de la dernière version | – |
| Source(s) | Bulletin de version de Kerio du 19 février 2008 |
| 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

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

2 Systèmes affectés

Kerio MailServer, versions 6.x.

3 Résumé

Plusieurs vulnérabilités affectent le serveur de courrier électronique *Kerio MailServer* et permettent à un utilisateur malveillant de contourner la politique de sécurité ou de provoquer un déni de service à distance.

4 Description

L'exploitation de plusieurs vulnérabilités dans le serveur et dans la console d'administration conduit à un arrêt inopiné (*crash*) ou un blocage (*deadlock*).

Une vulnérabilité affecte le greffon (*plug-in*) antivirus de *Visnetic*. Elle permet de provoquer un débordement de mémoire.

Une autre vulnérabilité, liée à la gestion des listes de contrôle d'accès, concerne le greffon antivirus *AVG*.

Une vulnérabilité affecte le décodage du format *uuencodé* et provoque une corruption de la mémoire.

L'exploitation de ces vulnérabilités permet à un utilisateur malveillant de contourner la politique de sécurité ou de provoquer un déni de service à distance.

5 Solution

La version 6.5.0 remédie à ces problèmes.

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

6 Documentation

– Bulletin de version *Kerio Mailserver* du 19 février 2008 :

http://www.kerio.com/kms_history.html

Gestion détaillée du document

20 février 2008 version initiale.