



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 23 mai 2006
N° CERTA-2006-AVI-210

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Cyrus IMAP Server

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-210>

Gestion du document

Référence	CERTA-2006-AVI-210
Titre	Vulnérabilité dans Cyrus IMAP Server
Date de la première version	23 mai 2006
Date de la dernière version	–
Source(s)	Mise à jour du projet Cyrus IMAP Server
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.

2 Systèmes affectés

Toutes les versions Cyrus IMAP Server antérieures à 2.3.3.

3 Résumé

Une vulnérabilité a été identifiée dans le module `popsubfolders` des différentes versions de Cyrus IMAP Server. Un utilisateur malveillant distant peut l'utiliser afin d'exécuter des commandes arbitraires sur la machine hébergeant le serveur Cyrus.

4 Description

IMAP (pour *Internet Message Access Protocol*) est un protocole pour accéder aux messages électroniques. Il faut pour cela contacter un serveur IMAP, tel que Cyrus IMAP Server. Une vulnérabilité de type débordement de mémoire a été identifiée dans le module `popsubfolders` (fichier `imap/pop3d.c`) de ce dernier. Il ne gère pas

correctement les noms d'utilisateurs lors du traitement de la commande USER. Une personne malveillante peut, à distance, utiliser cette vulnérabilité pour lancer des commandes arbitraires sur la machine hébergeant le serveur Cyrus.

5 Solution

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

6 Documentation

Mise à jour sur le site du projet Cyrus IMAP Server :
<http://asg.web.cmu.edu/cyrus/imapd/>

Gestion détaillée du document

23 mai 2006 version initiale.