Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 6 janvier 2003
N° CERTA-2002-AVI-280-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Cyrus IMAP Server

Gestion du document

Référence	CERTA-2002-AVI-280-001
Titre	Vulnérabilité de Cyrus IMAP Server
Date de la première version	26 décembre 2002
Date de la dernière version	6 janvier 2003
Source(s)	Avis de Sécurité DSA-215 de Debian
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

Cyrus IMAP Server versions 2.1.10 ou antérieures.

3 Résumé

Une vulnérabilité présente dans le serveur Cyrus IMAP permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance.

4 Description

Le serveur Cyrus IMAP permet à un utilisateur distant de récupérer ses messages électroniques via les protocoles `IMAP`, `POP3` ou `KPOP`.

Une vulnérabilité de type débordement de mémoire présente dans le serveur Cyrus IMAP permet, sous certaines conditions, à un utilisateur distant d'éxécuter du code arbitraire sur la machine hébergeant le serveur vulnérable.

Il est à noter que cette vulnérabilité est exploitable avant la phase d'authentification.

5 Solution

La version 2.1.11 de Cyrus IMAP Server corrige cette vulnérabilité.

6 Documentation

- Site de Cyrus IMAP Server :
  http://asg.web.cmu.edu/cyrus/imapd/
- Avis de sécurité DSA-215 de Debian :
  http://www.debian.org/security/2002/dsa-215
- Note VU#740169 du CERT/CC :
  http://www.kb.cert.org/vuls/id/740169
- Bulletin de sécurité SuSE-SA:2002:048 de SuSE :
  http://www.suse.com/de/security/2002_048_cyrus_imapd.html

Gestion détaillée du document

26 décembre 2002 version initiale.

6 janvier 2003 ajout référence au bulletin de sécurité SuSE-SA:2002:048 de SuSE.