Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 07 décembre 2004
N° CERTA-2004-AVI-379-004

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Cyrus Imap Serveur

Gestion du document

Référence	CERTA-2004-AVI-379-004
Titre	Multiples vulnérabilités dans Cyrus Imap Serveur
Date de la première version	23 novembre 2004
Date de la dernière version	07 décembre 2004
Source(s)	Avis de sécurité e-matters
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 ;
- exécution de code arbitraire à distance.

2 Systèmes affectés

`Cyrus Imap Server` version 2.x. Pour le détail des versions affectées par les différentes vulnérabilités voir la section Description.

3 Résumé

Plusieurs vulnérabilités présentes dans `Cyrus Imap Serveur` permettent à un utilisateur mal intentionné de réaliser un déni de service ou d'exécuter du code arbitraire à distance.

4 Description

`Cyrus Imap Server` est un serveur IMAP (Internet Message Access Protocol). Quatres vulnérabilités sont présentes sur ce serveur :

- Une vulnérabilité dans le traitement des commandes `PROXY` et `LOGIN` permet à un utilisateur mal intentionné, via l'utilisation d'un nom d'utilisateur malicieusement construit, de réaliser un déni de service ou d'exécuter du code arbitraire sur le système où se trouve le serveur vulnérable. Les versions 2.2.4 à 2.2.8 sont affectées par cette vulnérabilité.
- Une vulnérabilité dans le traitement d'un argument de la commande `PARTIAL` permet à un utilisateur mal intentionné de référencer une adresse mémoire externe au tampon. Les versions 2.2.6 et antérieures sont affectées par cette vulnérabilité.
- Une vulnérabilité dans le traitement d'un argument de la commande `FETCH` permet à un utilisateur mal intentionné de référencer une adresse mémoire externe au tampon. Les versions 2.2.8 et antérieures sont affectées par cette vulnérabilité.
- Une vulnérabilité dans la commande `APPEND` dûe à une erreur de programmation permet à un utilisateur mal intentionné de réaliser un déni de service ou d'exécuter du code arbitraire à distance. Les versions 2.2.7 et 2.2.8 sont affectées par cette vulnérabilité.

5 Solution

Mettre à jour le serveur avec la version 2.2.9 ou une version postérieure.

- Site internet de `Cyrus Imap Serveur` :
  http://ftp.andrew.cmu.edu/pub/cyrus-mail/

6 Documentation

- Bulletin de sécurité e-matters du 22 novembre 2004 :
  http://security.e-matters.de/advisories/152004.html
- Bulletin de sécurité FreeBSD du 22 novembre 2004 :
  http://www.vuxml.org/freebsd/
- Bulletin de sécurité Debian DSA-597 du 25 novembre 2004 :
  http://www.debian.org/security/2004/dsa-597
- Bulletin de sécurité Gentoo GLSA 200411-34 du 25 novembre 2004 :
  http://www.gentoo.org/security/en/glsa/glsa-200411-34.xml
- Bulletin de sécurité Mandrake MDKSA-2004:139 du 25 novembre 2004 :
  http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:139
- Bulletin de sécurité SuSE SUSE-SA:2004:043 du 03 décembre 2004 :
  http://www.suse.com/de/security/2004_43_cyrus_imapd.html
- Référence CVE CAN-2004-1011 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1011
- Référence CVE CAN-2004-1012 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1012
- Référence CVE CAN-2004-1013 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1013

Gestion détaillée du document

23 novembre 2004 version initiale.

25 novembre 2004 ajout de la référence au bulletin de sécurité Debian et aux références CVE.

25 novembre 2004 ajout de la référence au bulletin de sécurité Gentoo.

26 novembre 2004 ajout de la référence au bulletin de sécurité Mandrake.

07 décembre 2004 ajout de la référence au bulletin de sécurité SuSE.