

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Cyrus IMAPd

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-2011-AVI-505>

Gestion du document

Référence	CERTA-2011-AVI-505-001
Titre	Vulnérabilités dans Cyrus IMAPd
Date de la première version	13 septembre 2011
Date de la dernière version	20 septembre 2011
Source	Annonce de la version 2.4.11 de Cyrus IMAPd du 09 septembre 2011
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 ;
- déni de service à distance.

2 Systèmes affectés

Cyrus IMPAd 2.4.x.

3 Résumé

Cyrus IMAPd présentent des vulnérabilités permettant à un utilisateur malveillant, en particulier, l'exécution de code arbitraire à distance.

4 Description

Dans Cyrus IMAPd, deux vulnérabilités ont été corrigées :

- un débordement de zone mémoire est possible dans le serveur *nnTPd* et permet à un utilisateur malveillant d'exécuter du code arbitraire à distance ;

- dans certaines configurations, une erreur de gestion des pointeurs permet à un utilisateur malveillant de provoquer l'arrêt inopiné du serveur IMAPd. Cette vulnérabilité est exploitable à distance.

5 Solution

La version 2.4.11 de Cyrus IMAPd résoud ces problèmes.

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

6 Documentation

- Annonce de la version 2.4.11 de Cyrus IMAPd du 09 septembre 2011 :
http://www.cyrusimap.org/mediawiki/index.php/Latest_Updates
- Référence CVE CVE-2011-3208 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3208>
- Référence CVE CVE-2011-3481 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3481>

Gestion détaillée du document

13 septembre 2011 version initiale.

20 septembre 2011 ajout d'une deuxième vulnérabilité et de précisions sur la première.