

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples Vulnérabilités dans Cyrus IMAP

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-2005-AVI-087>

Gestion du document

Référence	CERTA-2005-AVI-087-001
Titre	Multiples Vulnérabilités dans Cyrus IMAP
Date de la première version	28 février 2005
Date de la dernière version	07 mars 2005
Source(s)	Bulletin de sécurité de l'université de Carnegie Mellon
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.

2 Systèmes affectés

Cyrus IMAP Server versions 2.x antérieures à la version 2.2.11.

3 Résumé

Plusieurs débordements de mémoire sont présents dans le serveur Cyrus IMAP. Ces vulnérabilités peuvent être exploitées par un utilisateur mal intentionné pour réaliser un déni de service ou exécuter du code arbitraire sur le système ayant le service vulnérable.

4 Description

Cyrus IMAP est un serveur de messagerie IMAP (Internet Message Access Protocol).

Cinq dépassements de tampon sont présents sur ce serveur. L'exploitation de ces vulnérabilités permet à un utilisateur mal intentionné de réaliser un déni de service ou d'exécuter du code arbitraire sur le système.

L'exploitation de certaines de ces vulnérabilités n'est possible que si l'utilisateur mal intentionné est authentifié.

5 Solution

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

6 Documentation

- Site internet du serveur Cyrus IMAP :
<http://asg.web.cmu.edu/cyrus/>
- Bulletin de sécurité de l'université de Carnegie Mellon :
<http://asg.web.cmu.edu/archive/message.php?mailbox=archive.info-cyrus&msg=33723>
- Bulletin de sécurité FreeBSD du 27 février 2005 :
<http://www.vuxml.org/freebsd/pkg-cyrus-imapd.html>
- Mise à jour NetBSD du 27 février 2005 :
<ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/mail/cyrus-imapd22/README.html>
- Bulletin de sécurité Suse du 24 février 2005 :
http://www.novell.com/linux/security/advisories/2005_09_cyrus_imapd.html
- Bulletin de sécurité Gentoo GLSA-200502-29 du 24 février 2005 :
<http://security.gentoo.org/glsa/glsa-200502-29.xml>
- Bulletin de sécurité Mandrake MDKSA-2005:051 du 4 mars 2005 :
<http://www.mandrakesoft.com/security/advisories?name=MDKSA-2005:051>
- Référence CVE CAN-2005-0546 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0205>

Gestion détaillée du document

28 février 2005 version initiale.

07 mars 2005 ajout des références CVE et du bulletin de sécurité Mandrake.