



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 10 juin 2005
N° CERTA-2005-AVI-097-002

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans UW-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-2005-AVI-097>

Gestion du document

Référence	CERTA-2005-AVI-097-002
Titre	Vulnérabilité dans UW-imapd
Date de la première version	02 mars 2005
Date de la dernière version	10 juin 2005
Source(s)	Bulletin de sécurité VU#702777 de l'US-CERT

TAB. 1 – Gestion du document

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

- Atteinte à la confidentialité des données ;
- contournement de l'authentification.

2 Systèmes affectés

UW-Imap versions antérieures à la version imap-2004b.

3 Résumé

Une vulnérabilité présente dans UW-Imap permet à un utilisateur mal intentionné d'accéder à la boîte aux lettres d'un utilisateur sans être authentifié.

4 Description

UW-Imap est le serveur de messagerie IMAP (Internet Message Access Protocol) créé par l'université de Washington.

Une vulnérabilité est présente dans le mécanisme d'authentification CRAM-MD5 (Challenge-Response Authentication Mechanism with MD5). Cette vulnérabilité permet à un utilisateur mal intentionné d'accéder à la boîte aux lettres d'un utilisateur sans être authentifié.

5 Solution

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

La version `imap-2004b` est disponible à l'adresse ci-dessous :
`ftp://ftp.cac.washington.edu/mail/imap.tar.Z`

6 Documentation

- Site Internet du serveur UW-Imap :
`http://www.washington.edu/imap/`
- Bulletin de sécurité VU#702777 de l'US-CERT du 27 janvier 2005 :
`http://www.kb.cert.org/vuls/id/702777`
- Bulletin de sécurité de SUSE du 01 mars 2005 :
`http://www.novell.com/linux/security/advisories/2005_12_imap.html`
- Bulletin de sécurité Gentoo GLSA 200502-02 du 02 février 2005 :
`http://www.gentoo.org/security/en/glsa/glsa-200502-02.xml`
- Bulletin de sécurité Mandrake MDKSA-2005:026 du 01 février 2005 :
`http://www.mandriva.com/security/advisories?name=MDKSA-2005:026`
- Bulletin de sécurité Red Hat RHSA-2005:128 du 23 février 2005 :
`http://rhn.redhat.com/errata/RHSA-2005-128.html`
- Mise à jour de sécurité du paquetage NetBSD `imap-uw` :
`ftp://ftp.netbsd.org/pub/NetBSD/packages/pkgsrc/mail/imap-uw/README.html`
- Bulletin de sécurité FreeBSD "imap-uw – authentication bypass when CRAM-MD5 is enabled" du 03 juin 2005 :
`http://www.vuxml.org/freebsd`
- Référence CVE CAN-2005-0198 :
`http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0198`

Gestion détaillée du document

02 mars 2005 version initiale.

03 mars 2005 ajout de la référence au bulletin de sécurité NetBSD.

10 juin 2005 ajout des références aux bulletins de sécurité Gentoo, Mandrake, Red Hat, FreeBSD.