Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 04 avril 2003
N° CERTA-2003-AVI-055-003

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du client de messagerie Mutt

Gestion du document

Référence	CERTA-2003-AVI-055-003
Titre	Vulnérabilité du client de messagerie Mutt
Date de la première version	21 mars 2003
Date de la dernière version	04 mars 2003
Source(s)	Bulletin de sécurité CORE-20030304-02 de CORELABS
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 ;
- déni de service.

2 Systèmes affectés

- Versions de Mutt antérieures ou égales à la version 1.4.0 (stable) ;
- versions de Mutt antérieures ou égales à la version 1.5.3 (instable).

3 Résumé

Une vulnérabilité présente dans le client de messagerie Mutt peut être exploitée afin d'exécuter du code arbitraire sur la plate-forme vulnérable.

4 Description

Mutt est un client de messagerie très utilisé sur les plates-formes Linux. Il supporte les protocoles POP3 (Post Office Protocol) et IMAP (Internet Message Access Protocol) pour l'interrogation des serveurs de messagerie.

Une vulnérabilité de type débordement de mémoire est présente dans la routine de traitement des noms de dossiers sous IMAP.

Un utilisateur mal intentionné administrant un serveur de messagerie IMAP peut exploiter cette vulnérabilité pour exécuter du code arbitraire à distance sur la plate-forme cliente avec les privilèges du compte utilisant l'application Mutt.

5 Solution

Installer la version 1.4.1 ou 1.5.4 de Mutt :
http://www.mutt.org

ou appliquer le correctif de l'éditeur :

- Bulletin de sécurité SuSE SuSE-SA:2003:020 :
  http://www.suse.de/de/security/2003_020_mutt.html
- Bulletin de sécurité Gentoo GLSA:mutt(200303-19) :
  http://www.gentoo.org
- Bulletin de sécurité DSA-268 de Debian :
  http://www.debian.org/security/2003/dsa-268
- Bulletin de sécurité MDKSA-2003:041 de Mandrake :
  http://www.mandrakesecure.net/en/advisories/advisory.php?name=MDKSA-2003:041
- Bulletin de sécurité RHSA-2003:109 de Red Hat :
  http://rhn.redhat.com/errata/RHSA-2003-109.html

6 Documentation

- Bulletin de sécurité CORE-20030304-02 "Mutt controlled IMAP server buffer overflow" de CORELABS :
  http://www.coresecurity.com/common/showdoc.php?idx=310&idxseccion=10
- Référence CVE CAN-2003-0140 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0140

Gestion détaillée du document

21 mars 2003 version initiale.
25 mars 2003 Ajout des bulletins de sécurité SuSE et Gentoo.
27 mars 2003 Ajout bulletin de sécurité Debian. Ajout référence CVE.
04 avril 2003 Ajout bulletins de sécurité Mandrake et Red Hat.