



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 30 août 2004
N° CERTA-2004-AVI-276-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Courier-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-2004-AVI-276>

Gestion du document

Référence	CERTA-2004-AVI-276-001
Titre	Vulnérabilité dans Courier-IMAP
Date de la première version	25 août 2004
Date de la dernière version	30 août 2004
Source(s)	Avis de sécurité iDefense
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

- Courier Mail Server 0.x ;
- Courier-IMAP versions 1.x ;
- Courier-IMAP versions 2.x.

3 Résumé

Une vulnérabilité présente dans Courier-IMAP peut être exploitée par un utilisateur mal intentionné pour réaliser un déni de service ou exécuter du code arbitraire.

4 Description

Courier-IMAP est un serveur de mail IMAP/POP.

Une vulnérabilité de type « chaîne de format » (`format string`) est présente dans la fonction `auth_debug()` utilisée pour le débogage du `login` dans le logiciel Courier-IMAP.

Ce débogage n'est pas activé par défaut.

5 Contournement provisoire

Désactiver le mode de débogage du `login` en mettant le paramètre `DEBUG_LOGIN=0` dans le fichier de configuration.

6 Solution

Mettre à jour Courier-IMAP avec la version 3.0.7.

7 Documentation

- Bulletin de sécurité de iDefense du 18 août 2004 :
<http://www.iddefense.com/application/poi/display?id=131&type=vulnerabilities>
- Bulletin de sécurité Gentoo GLSA 200408-19 du 19 août 2004 :
<http://www.gentoo.org/security/en/glsa/glsa-200408-19.xml>
- Bulletin de sécurité FreeBSD pour courier-imap du 22 août 2004 :
<http://www.vuxml.org/freebsd>
- Référence CVE CAN-2004-0777 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0777>

Gestion détaillée du document

25 août 2004 version initiale.

30 août 2004 ajout des références aux bulletins de sécurité Gentoo et FreeBSD ainsi que de la référence CVE.