

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Courier

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-494>

Gestion du document

Référence	CERTA-2005-AVI-494
Titre	Vulnérabilité de Courier
Date de la première version	19 décembre 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité Debian DSA-917 du 08 décembre 2005
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

Contournement de la politique de sécurité.

2 Systèmes affectés

Courier Mail Server versions 0.52.1 et antérieures.

3 Résumé

Une vulnérabilité dans le serveur de messagerie Courier permet à un utilisateur distant mal intentionné de contourner la politique de sécurité du système.

4 Description

Une erreur dans le service d'authentification *courier-authdaemon* du serveur de messagerie Courier empêche une vérification correcte des utilisateurs autorisés à se connecter. Ainsi, il est possible d'utiliser le service de messagerie même avec un compte désactivé. Un utilisateur mal intentionné peut utiliser un compte de ce type pour se connecter frauduleusement à distance.

5 Solution

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

6 Documentation

- Bulletin de sécurité Debian DSA 917 du 08 décembre 2005 :
<http://www.debian.org/security/dsa-917>
- Bulletin de sécurité Ubuntu USN-226-1 du 09 décembre 2005 :
<http://www.ubuntulinux.org/usn/usn-226-1>
- Référence CVE CAN-2005-3532 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-3532>

Gestion détaillée du document

19 décembre 2005 version initiale.