

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de GNU mailutils

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-350>

Gestion du document

Référence	CERTA-2005-AVI-350-001
Titre	Vulnérabilité de GNU mailutils
Date de la première version	19 septembre 2005
Date de la dernière version	10 octobre 2005
Source(s)	Bulletin de sécurité iDEFENSE Security Advisory 09.09.05
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 à distance par un utilisateur authentifié.

2 Systèmes affectés

GNU mailutils version 0.6 et versions antérieures.

3 Résumé

Une vulnérabilité dans GNU mailutils permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance sur la plate-forme vulnérable.

4 Description

GNU mailutils est un ensemble d'utilitaires relatifs au courrier électronique. Parmi ces utilitaires, on peut citer le serveur IMAP `imap4d`.

Une vulnérabilité de type débordement de mémoire dans le serveur `imap4d` lors du traitement de requêtes IMAP SEARCH permet à un utilisateur authentifié mal intentionné d'exécuter du code arbitraire à distance sur la plate-forme vulnérable.

5 Solution

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

6 Documentation

- Site Internet de GNU mailutils :
<http://www.gnu.org/software/mailutils/mailutils.html>
- Bulletin de sécurité iDEFENSE Security Advisory 09.09.05 :
<http://www.odefense.com/application/poi/display?id=303&type=vulnerabilities>
- Bulletin de sécurité Gentoo 200509-10 / mailutils du 17 septembre 2005 :
<http://www.gentoo.org/security/en/glsa/glsa-200509-10.xml>
- Bulletin de sécurité Debian DSA-841 du 04 octobre 2005 :
<http://www.debian.org/security/2005/dsa-841>
- Référence CVE CAN-2005-2878 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2878>

Gestion détaillée du document

19 septembre 2005 version initiale.

10 octobre 2005 ajout de la référence au bulletin de sécurité Debian DSA-841 et de la référence CVE CAN-2005-2878.