



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 29 septembre 2004
N° CERTA-2004-AVI-328

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Sendmail avec SASL

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-328>

Gestion du document

Référence	CERTA-2004-AVI-328
Titre	Vulnérabilité dans Sendmail avec SASL
Date de la première version	29 septembre 2004
Date de la dernière version	–
Source(s)	Bulletin de sécurité DSA-554-1 de Debian
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

- Les versions de sendmail antérieures à 8.12.3-71 avec la distribution Debian stable (woody);
- les versions de sendmail antérieures à 8.13.1-13 avec la distribution Debian unstable (sid).

3 Description

SASL (Simple Authentication and Security Layer) est un mécanisme permettant d'ajouter des fonctionnalités d'authentification à des protocoles réseau.

L'installation du package `sasl-bin`, pour intégrer SASL dans le serveur de messagerie sendmail, emploie un compte possédant un mot de passe par défaut. Cette vulnérabilité peut permettre à un utilisateur mal intentionné d'employer le serveur de messagerie comme relais ouvert afin d'envoyer des méls non sollicités.

4 Solution

Appliquer le correctif fourni par l'éditeur (cf. Documentation).

5 Documentation

- Bulletin de sécurité DSA-554-1 de Debian :
<http://www.debian.org/security/2004/dsa-554>
- Référence CVE CAN-2004-0833 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0833>

Gestion détaillée du document

29 septembre 2004 version initiale.