Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 17 janvier 2006
N° CERTA-2006-AVI-031

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du serveur de fax HylaFAX

Gestion du document

Référence	CERTA-2006-AVI-031
Titre	Vulnérabilité du serveur de fax HylaFAX
Date de la première version	17 janvier 2006
Date de la dernière version	–
Source(s)	
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 ;
- contournement de la politique de sécurité ;
- élévation de privilèges.

2 Systèmes affectés

Tout système Unix utilisant le serveur de fax `HylaFAX` version 4 dont les sources sont antérieures ou égales à la révision 4.2.3.

3 Résumé

`HylaFAX` fournit un service permettant l'envoi et la réception de fax pour les utilisateurs autorisés à se connecter au serveur.

Deux vulnérabilités combinées permettent à un utilisateur distant non authentifié d'exécuter du code arbitraire avec les privilèges du service.

4 Description

Lorsque le service d'authentification modulaire PAM est inactif n'importe quel mot de passe valide l'authentification. Dans ce cas, un utilisateur distant quelconque peut accéder au service (CAN-2005-3538).

Un script ne validant pas les entrées utilisateur, peut donc être détourné pour exécuter des commandes arbitraires (CAN-2005-3539).

5 Contournement provisoire

Filtrer les adresses IP autorisées à se connecter à l'aide d'un pare-feu en coupure (ports 444/tcp, 4457/tcp et 4459/tcp par défaut).

6 Solution

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

7 Documentation

- Site officiel de HylaFAX :
  http://www.hylafax.org/
- Bulletin de sécurité Debian DSA 933 du 09 janvier 2006 :
  http://www.debian.org/security/2006/dsa-933
- Bulletin de sécurité Gentoo GLSA-200601-03 du 06 janvier 2006 :
  http://www.gentoo.org/security/en/glsa/glsa-200601-03.xml
- Bulletin de sécurité Mandriva MDKSA-2006:015 du 16 janvier 2006 :
  http://wwwnew.mandriva.com/security/advisories?name=MDKSA-2006:015
- Référence CVE CAN-2005-3538 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-3538
- Référence CVE CAN-2005-3539 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-3539

Gestion détaillée du document

17 janvier 2006 version initiale.