Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 20 janvier 2005
N° CERTA-2005-AVI-021

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans la configuration du serveur de fax HylaFAX

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-021

Gestion du document

Référence	CERTA-2005-AVI-021
Titre	Vulnérabilité dans la configuration du serveur de fax HylaFAX
Date de la première version	20 janvier 2005
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

Contournement de la politique de sécurité.

2 Systèmes affectés

Tout système Unix utilisant le serveur de fax *HylaFAX* version 4 dont les sources sont antérieures ou égales à la révision 4.2.0.

3 Résumé

HylaFAX fournit un service permettant l'envoi et la réception de fax pour les utilisateurs autorisés à se connecter au serveur. Une mauvaise gestion des restrictions d'accès permet à un utilisateur mal intentionné d'user de ce service à son profit.

4 Description

Le fichier de configuration *host.hfaxd* permet de spécifier les hôtes et ou utilisateurs autorisés à utiliser le service. Certaines entrées, couramment présentes par défaut, peuvent être incorrectement interprétées comme un nom d'utilisateur au lieu d'un nom d'hôte et donc être utilisées pour fournir un accès à un utilisateur mal intentionné.

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

Utiliser les sources de *HylaFAX* en version 4.2.1 au moins ou se référer au bulletin de sécurité de l'éditeur.

7 Documentation

- Site officiel de *HylaFAX* :
  http://www.hylafax.org
- Bulletin de sécurité Secunia 13812 du 12 janvier 2005 :
  http://secunia.com/advisories/13812/
- Bulletin de sécurité Mandrake MDKSA-2005:006 du 12 janvier 2005 :
  http://www.mandrakesoft.com/security/advisories?name=MDKSA-2005:006
- Bulletin de sécurité Debian DSA-634 du 11 janvier 2005 :
  http://www.debian.org/security/2005/dsa-634
- Bulletin de sécurité Gentoo GLSA-200501-21 du 11 janvier 2005 :
  http://www.gentoo.org/security/en/glsa/glsa-200501-21.xml
- Référence CVE CAN-2004-1182 du 13 décembre 2004 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1182

Gestion détaillée du document

20 janvier 2005 version initiale.