Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 30 août 2002
N° CERTA-2002-AVI-196

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilite de HylaFAX

Gestion du document

Référence	CERTA-2002-AVI-196
Titre	Vulnérabilite de HylaFAX
Date de la première version	30 août 2002
Date de la dernière version	–
Source(s)	Avis de securité de Mandrake
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.

2 Systèmes affectés

Toutes les versions de `HylaFAX` antérieures à la version 4.1.3.

3 Résumé

Plusieurs vulnérabilités dans le paquetage `HylaFAX` permettent à un utilisateur mal intentionné d'exécuter du code arbitraire à distance.

4 Description

`HylaFAX`, organisé autour d'une architecture client-serveur, permet l'envoi et la reception de fax. Plusieurs utilitaires du paquetage possèdent des vulnérabilités de type débordement de mémoire permettant l'exécution de code arbitraire : `faxgetty`, `faxrm`, `faxalter`, `faxstat`, `faxwatch`, `sendfax`, `sendpage`.

5 Solution

Installer `HylaFAX` version 4.1.3 (cf. section documentation).

6 Documentation

Avis de sécurité de Mandrake Linux MDKSA-2002:055 :
http://www.linux-mandrake.com/en/updates/2002/MDKSA-2002-055.php

Gestion détaillée du document

30 août 2002 version initiale.