



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 19 octobre 2000
N° CERTA-2000-AVI-062

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans lpspool et ftpd sous HP-UX

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-2000-AVI-062>

Gestion du document

Référence	CERTA-2000-AVI-062
Titre	Vulnérabilités dans lpspool et ftpd sous HP-UX
Date de la première version	19 octobre 2000
Date de la dernière version	–
Source(s)	Avis du CIAC Bugtraq
Pièce(s) jointe(s)	Aucune

TAB. 1 – gestion du document

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risques

- Augmentation des privilèges, déni de service pour lpspooler.
- Accès root pour ftpd.

2 Systèmes affectés

Pour *lpspooler* les versions vulnérables d'HP-UX sont :

- HP-UX 11.00;
- HP-UX 10.20;
- HP-UX 10.10;
- HP-UX 10.01.

Pour *ftpd*, les versions vulnérables sont :

- HP-UX 11.04;
- HP-UX 11.00;

- HP-UX 10.24;
- HP-UX 10.20;
- HP-UX 10.10;
- HP-UX 10.01.

3 Résumé

De multiples vulnérabilités sont présentes dans les services *lpspooler* et *ftpd* du système HP-UX.

4 Description

Des débordements de mémoire dans *lpspooler* (plus précisément `PrinterMgmt.LP-SPOOL`) permettent à un utilisateur mal intentionné d'augmenter ses privilèges, ou d'arrêter le service d'impression.

Sous les versions d'HP-UX 11.0x seulement, l'installation par défaut du service FTP permet la commande `SITE EXEC` permettant à un utilisateur distant d'obtenir les privilèges root sur le serveur.

Dans toutes les versions d'HP-UX 11.0x et 10.xx, le *daemon* `ftpd` passe à la fonction `setproctitle()` des paramètres avec un format incorrect, permettant ainsi à l'utilisateur mal intentionné d'obtenir les privilèges de root sur la machine.

5 Solution

Télécharger les correctifs depuis le site HP :

<http://itrc.hp.com>

- Pour *lpspooler* :

- pour HP-HX 11.00 appliquer le correctif nommé PHCO_22365,
- pour HP-HX 10.20 appliquer le correctif nommé PHCO_22364,
- pour HP-HX 10.10 appliquer le correctif nommé PHCO_22411,
- pour HP-HX 10.01 appliquer le correctif nommé PHCO_22410.

Pour *ftpd* :

- pour HP-HX 11.00 appliquer le correctif nommé PHNE_22936,
- pour HP-HX 11.04 appliquer le correctif nommé PHNE_22060,
- pour HP-HX 10.20 appliquer le correctif nommé PHNE_22057,
- pour HP-HX 10.24 appliquer le correctif nommé PHNE_22059,
- pour HP-HX 10.01 et 10.10 appliquer le correctif nommé PHNE_22058.

6 Documentation

- L'avis d'HP est visible sur le site :

<http://itrc.hp.com>

- le CIAC a publié ces deux avis dans un seul page sur son site :

<http://www.ciac.org/ciac/bulletins/l-006.shtml>

Gestion détaillée du document

19 octobre 2000 version initiale.