



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 octobre 2003
N° CERTA-2003-AVI-163

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de dtprintinfo 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-2003-AVI-163>

Gestion du document

Référence	CERTA-2003-AVI-163
Titre	Vulnérabilité de dtprintinfo sous HP-UX
Date de la première version	13 octobre 2003
Date de la dernière version	–
Source(s)	Bulletin de sécurité HPSBUX0310-289 de Hewlett-Packard
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

Elévation de privilèges.

2 Systèmes affectés

HP-UX versions B.11.00, B.11.11 et B.11.22.

3 Description

La commande `dtprintinfo` permet de visualiser les files d'impression.

Une vulnérabilité de type débordement de mémoire présente dans une routine manipulant la variable d'environnement `DISPLAY` peut être exploitée par un utilisateur mal intentionné afin d'obtenir les privilèges du super-utilisateur `root`.

Cette vulnérabilité n'est exploitable qu'en local.

4 Contournement provisoire

Dans l'attente de l'application du correctif, retirer le drapeau "`setuid`" de l'exécutable `/usr/dt/bi/dtprintinfo`.

5 Solution

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

6 Documentation

Bulletin de sécurité HPSBUX0310-289 "Potential Security Vulnerability in dtprintf" de Hewlett-Packard :
<http://itrc.hp.com>

Gestion détaillée du document

13 octobre 2003 version initiale.