Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 23 janvier 2004
N° CERTA-2004-AVI-016

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités 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-2004-AVI-016

Gestion du document

Référence	CERTA-2004-AVI-016
Titre	Multiples vulnérabilités sous HP-UX
Date de la première version	23 janvier 2004
Date de la dernière version	–
Source(s)	Bulletin de sécurité HPSBUX0401-308 de Hewlett-Packard Bulletin de sécurité HPSBUX0401-310 de Hewlett-Packard Bulletin de sécurité HPSBUX0401-312 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 ;
- exécution de code arbitraire à distance ;
- déni de service.

2 Systèmes affectés

- HP-UX 11.0, HP-UX 11.04, HP-UX 11.11 (vulnérabilité dans `calloc()`) ;
- HP-UX 11.0, HP-UX 11.04, HP-UX 11.11, HP-UX 11.22 (vulnérabilité dans `libDtSvc`) ;
- HP-UX 11.0, HP-UX 11.1 (vulnérabilité dans `rwrite`).

3 Résumé

Hewlett-Packard a publié plusieurs bulletins concernant des vulnérabilités sous HP-UX.

4 Description

Une vulnérabilité est présente dans la fonction `calloc()`. Un utilisateur mal intentionné peut exploiter cette vulnérabilité au travers d'une application qui utiliserait cette fonction afin d'exécuter du code arbitraire, en local ou à distance, sur une plate-forme vulnérable.

Des vulnérabilités sont également présentes dans la commande `/usr/lbin/rwrite` ou la bibliothèque `libDtSvc`. L'exploitation d'une de ces vulnérabilités peut permettre à un utilisateur local de réaliser une élévation de privilèges (obtention des privilèges du super-utlisateur `root`).

5 Solution

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

6 Documentation

- Bulletin de sécurité HPSBUX0401-308 "SSRT3492 libDtSvc" de Hewlett-Packard : http://itrc.hp.com
- Bulletin de sécurité HPSBUX0401-312 "SSRT3556 /usr/lbin/rwrite" de Hewlett-Packard : http://itrc.hp.com
- Bulletin de sécurité HPSBUX0401-310 "SSRT2341 calloc(3c) in HP-UX" de Hewlett-Packard : http://itrc.hp.com

Gestion détaillée du document

23 janvier 2004 version initiale.