Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 05 août 2004
N° CERTA-2003-AVI-183-003

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de libDtHelp (CDE)

Gestion du document

Référence	CERTA-2003-AVI-183-003
Titre	Vulnérabilité de libDtHelp (CDE)
Date de la première version	12 novembre 2003
Date de la dernière version	05 août 2004
Source(s)	Bulletin de sécurité #57414 de Sun Note VU#575804 du CERT/CC
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

- Déni de service ;
- élévation de privilèges.

2 Systèmes affectés

- Solaris 7,8 et 9 pour les architectures Sparc et x86;
- HP-UX 11.00 et 11.11;
- HP Tru64 UNIX V5.1.

3 Résumé

Une vulnérabilité présente dans la bibliothèque libDtHelp de CDE (Common Desktop Environment) peut être exploitée par un utilisateur mal intentionné afin de réaliser une élévation de privilèges.

4 Description

CDE (Common Desktop Environment) est une interface graphique utilisée notamment sur les plates-formes Solaris.

En manipulant la variable d'environnement `DTHELPUSERSEARCHPATH`, un utilisateur mal intentionné peut exploiter une vulnérabilité de type débordement de mémoire présente dans la bibliothèque libDtHelp de CDE afin d'exécuter du code arbitraire.

Avec certains utilitaires tels que `dtprintinfo` possédant le drapeau `suid`, l'exploitation de cette vulnérabilité permet d'obtenir les privilèges du super-utilisateur `root`.

Cette vulnérabilité n'est exploitable qu'en local.

5 Solution

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

6 Documentation

- Bulletin de sécurité #57414 de Sun :
  http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F57414
- Bulletin de sécurité HPSBUX0311-297 de Hewlett-Packard :
  http://itrc.hp.com
- Bulletin de sécurité SSRT3657-Tru64 de Hewlett-Packard :
  http://itrc.hp.com
- Bulletin de sécurité de SGI 20040801-01-P du 01 août 2004 :
  ftp://patches.sgi.com/support/free/security/advisories/20040801-01-P.asc
- Note VU#575804 du CERT/CC :
  http://www.kb.cert.org/vuls/id/575804
- Référence CVE CAN-2003-0834 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0834

Gestion détaillée du document

12 novembre 2003 version initiale.
18 novembre 2003 ajout référence au bulletin de HP.
04 décembre 2003 ajout référence au bulletin de sécurité SSRT3657-Tru64.
05 août 2004 ajout référence au bulletin de sécurité SGI.