

Affaire suivie par :  
CERTA

## BULLETIN D'ALERTE DU CERTA

### Objet : Exploitation massive d'une faille de CDE

---

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-2002-ALE-001>

---

### Gestion du document

|                             |  |
|-----------------------------|--|
| Référence                   | CERTA-2002-ALE-001                       |
| Titre                       | Exploitation massive d'une faille de CDE |
| Date de la première version | 24 janvier 2002                          |
| Date de la dernière version | -  |
| Source(s)                   | Avis du CERT/CC CA-2002-01               |
| 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

Compromission du système.

## 2 Systèmes affectés

Tous les systèmes utilisant CDE (Common Desktop Environment).

## 3 Résumé

Une vulnérabilité du démon `dtspcd` sous CDE, décrite dans l'avis CERTA-2001-AVI-139, est massivement exploitée.

## 4 Description

Le démon `dtspcd` permet d'exécuter des applications à distance. Ce démon est par défaut en écoute sur le port 6112/tcp. Une vulnérabilité de ce démon récemment découverte est actuellement exploitée pour prendre le contrôle de machines à distance. Les symptômes d'une compromission par cette faille peuvent être l'ajout de fichiers dans

le répertoire `/usr/lib/` (par exemple, le fichier `/usr/lib/libcnetix.a`), ainsi que dans le répertoire `/tmp/` (par exemple, le fichier `/tmp/.fakex`), ou encore des connexions `rsh` sortantes intempestives.

## 5 Contournement provisoire

Filtrer le port `6112/tcp` au niveau du garde-barrière. Si le service `dtspc` n'est pas nécessaire, le désactiver dans le fichier `/etc/inetd.conf`. Sinon, paramétrer `tcp-wrappers` pour n'autoriser que certaines machines à se connecter à ce service.

## 6 Solution

Mettre en place les correctifs proposés par votre éditeur.

## 7 Documentation

Avis du CERT/CC :

<http://www.cert.org/advisories/CA-2002-01.html>

## Gestion détaillée du document

24 janvier 2002 version initiale.