Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 24 janvier 2002
N° CERTA-2002-ALE-001

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Exploitation massive d'une faille de CDE

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/libchetnix.a`), ainsi que dans le répertoire `/tmp/` (par exemple, le fichier `/tmp/.fakex`), ou encore des connexions `rcp` 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, paramètrer `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.