Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 27 mars 2002
N° CERTA-2001-AVI-139-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de CDE

Gestion du document

Référence	CERTA-2001-AVI-139-001
Titre	Vulnérabilité de CDE
Date de la première version	13 novembre 2001
Date de la dernière version	27 mars 2002
Source(s)	Avis CA-2001-31 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 ;
- exécution de code arbitraire.

2 Systèmes affectés

Systèmes sur lesquels est lancé le service `CDE Subprocess Control Service`.

3 Résumé

Une vulnérabilté dans le démon `CDE Subprocess Control Service` permet à un utilisateur mal intentionné d'exécuter du code arbitraire sur la machine avec les droits de l'utilisateur *root*.

L'exploitation de cette vulnérabilité peut se faire en local ou à distance.

4 Description

CDE (Common Desktop Environment) est une interface graphique des systèmes UNIX et Linux. Le démon `CDE Subprocess Control Service` (`dtspcd`) est un démon réseau qui accepte des requêtes de clients pour exécuter ou lancer des applications à distance. Le démon dtspcd tourne par défaut sur le port 6112/tcp avec les droits de l'utilisateur *root*.

Une vulnérabilité de type débordement de mémoire permet à un utilisateur mal intentionné d'exécuter du code arbitraire sur la machine avec les droits de l'utilisateur *root*.

5 Contournement provisoire

Pour éviter une attaque venant de l'extérieur, limitez l'accès au demon `dtspcd` au niveau des gardes-barrières (port 6112/tcp par défaut).

6 Solution

Consultez votre éditeur pour obtenir une mise à jour suivant votre distribution.

7 Documentation

L'environnement CDE :
http://www.opengroup.org/cde
L'avis de sécurité du CERT-CC :
http://www.cert.org/advisories/CA-2001-31.html
L'avis de sécurité SGI :
ftp://patches.sgi.com/support/free/security/advisories/20020302-01-A

Gestion détaillée du document

13 novembre 2001 version initiale.
27 mars 2002 première révision : ajout de l'avis SGI.