Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 18 septembre 2002
N° CERTA-2002-AVI-147-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités de CDE Tooltalk

Gestion du document

Référence	CERTA-2002-AVI-147-001
Titre	Vulnérabilités de CDE Tooltalk
Date de la première version	11 juillet 2002
Date de la dernière version	18 septembre 2002
Source(s)	Avis du CERT/CC CA-2002-20 Avis 46022 de Sun
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 à distance.

2 Systèmes affectés

Tous les systèmes utilisant `CDE Tooltalk` (`rpc.ttdbserverd`).

3 Résumé

Deux vulnérabilités de `CDE Tooltalk` (`rpc.ttdbserverd`) permettent à un utilisateur mal intentionné de réaliser un déni de service ou d'exécuter du code arbitraire sur le système à distance.

4 Description

CDE (Common Desktop Environment) est une interface graphique qui fonctionne sous les systèmes UNIX et Linux. CDE Tooltalk est un système de gestion des messages qui permet aux applications de communiquer entre elles sur des machines différentes.

Deux vulnérabilités de CDE Tooltalk permettent à un utilisateur mal intentionné de réaliser un déni de service ou d'exécuter du code arbitraire à distance.

La première de ces vulnérabilités concerne la procédure _TT_ISCLOSE(). Cette procédure ne contrôle pas les paramètres passés en argument, ce qui permet d'écrire en mémoire.

La seconde vulnérabilité concerne les opérations sur les fichiers. Il est possible d'écraser n'importe quel fichier du système en référençant des liens symboliques.

5 Contournement provisoire

Désactiver rpc.ttdbserverd si ce service n'est pas nécessaire.
Filtrer les ports 111/tcp, 111/udp et 32773/tcp au niveau du garde-barrière.

6 Solution

Appliquer les correctifs indiqués dans le bulletin de sécurité 46022 de Sun (voir Documentation).

7 Documentation

Avis du CERT/CC CA-2002-20 :
http://www.cert.org/advisories/CA-2002-20.html
Avis 46022 de Sun :
http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F46022

Gestion détaillée du document

11 juillet 2002 version initiale.
18 septembre 2002 ajout du lien vers les correctifs de Sun.