



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 17 septembre 2002  
N° CERTA-2002-AVI-173-001

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité de ToolTalk

---

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-AVI-173>

---

### Gestion du document

Référence	CERTA-2002-AVI-173-001
Titre	Vulnérabilité de ToolTalk
Date de la première version	13 août 2002
Date de la dernière version	17 septembre 2002
Source(s)	Avis CA-2002-26 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

- Elévation de privilèges ;
- déni de service.

## 2 Systèmes affectés

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

Une liste des systèmes vulnérables est publiée dans le document VU#387387 du CERT/CC (cf. section documentation).

## 3 Résumé

Une vulnérabilité présente dans CDE ToolTalk(`rpc.ttdbserverd`) permet à un utilisateur mal intentionné d'exécuter du code arbitraire, à distance, avec les privilèges de l'administrateur système (`root`).

## 4 Description

CDE (Common Desktop Environment) est une interface graphique livrée sur différents systèmes UNIX. Cette interface utilise le service ToolTalk, basé sur les RPC, pour la communication inter-applications.

Une vulnérabilité de type débordement de mémoire présente dans le traitement des arguments passés à la procédure `_TT_CREATE_FILE()` permet à un utilisateur mal intentionné d'exécuter du code arbitraire, à distance, avec les privilèges de l'administrateur système (`root`).

## 5 Contournement provisoire

- Désactiver le service `rpc.ttdbserverd` si ce service n'est pas nécessaire ;
- filtrer les ports 111/tcp, 111/udp et le port utilisé par `rpc.ttdbserverd` au niveau du garde-barrière afin d'empêcher l'exploitation de la vulnérabilité depuis l'Internet.

## 6 Solution

Consulter le site de l'éditeur pour connaître la disponibilité des correctifs.

## 7 Documentation

- Avis CA-2002-26 "Buffer Overflow in CDE ToolTalk" du CERT/CC :  
<http://www.cert.org/advisories/CA-2002-26.html>
- Note VU#387387 "ToolTalk vulnerable to buffer overflow via `_TT_CREATE_FILE()`" :  
<http://www.kb.cert.org/vuls/id/387387>
- Bulletin Alert Notification #46366 "Buffer Overflow in the ToolTalk Library" :  
[http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F46366&zone\\_32=category%3Asecurity](http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F46366&zone_32=category%3Asecurity)

## Gestion détaillée du document

**13 août 2002** version initiale.

**17 septembre 2002** Ajout Bulletin Alert Notification #46366 de Sun.