Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 23 juillet 2004
N° CERTA-2004-AVI-253

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du service RPC DCE

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-2004-AVI-253

Gestion du document

Référence	CERTA-2004-AVI-253
Titre	Vulnérabilité du service RPC DCE
Date de la première version	23 juillet 2004
Date de la dernière version	–
Source(s)	Bulletins de sécurité HP HPSBUX0311-299, HPSBTU01051 et HPSB0V01056
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

- Exécution de commande arbitraire à distance ;
- déni de service.

2 Systèmes affectés

- HP-UX 11 ;
- HP Tru64 ;
- HP OpenVMS.

3 Résumé

Une vulnérabilité présente dans le service RPC DCE (`dced`) peut être exploitée par un utilisateur mal intentionné afin de réaliser un déni de service ou d'exécuter du code arbitraire à distance.

4 Description

Le service `dced` est l'implementation du service RPC DCE (Distributed Computing Environment) endpoint mapper (`epmap`) sous HP; DCE étant un ensemble de service et d'outils qui permettent la création et le déploiement d'applications distibuées.

Un débordement de mémoire est présent dans le service `dced` en écoute par défaut sur le port `135/tcp`. L'exploitation de cette vulnérabilité permet à un utilisateur mal intentionné d'exécuter du code arbitraire à distance avec les privilèges de l'utilisateur sous lequel le service a été démarré; par défaut les privillèges du super utilisateur (`root`).

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité concernant HP-UX 11.x (HPSBUX0311-299) :
  http://www2.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBUX0311-299
- Bulletin de sécurité concernant HP-UX Tru64 (HPSBTU01051) :
  http://www2.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBTU01051
- Bulletin de sécurité concernant HP OpenVMS (HPSB0V01056) :
  http://www2.itrc.hp.com/service/cki/docDisplay.do?docId=HPSB0V01056

Gestion détaillée du document

23 juillet 2004 version initiale.