



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 avril 2002
N° CERTA-2002-AVI-080

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités sous TRUE64 UNIX

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-080>

Gestion du document

Référence	CERTA-2002-AVI-080
Titre	Multiples vulnérabilités sous TRUE64 UNIX
Date de la première version	17 avril 2002
Date de la dernière version	–
Source(s)	Avis de sécurité SSRT-541 de Compaq
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

True64 UNIX versions 4.0f à 5.1a.

3 Description

Compaq a publié un avis de sécurité décrivant plusieurs vulnérabilités de CDE (Common Desktop Environment), NFS (Network File System), NIS (Network Information Service) et de la bibliothèque libc :

- CDE : de multiples débordements mémoire dans différentes commandes ou services (dtaction, tsession, dt-printinfo, dtspcd) permettent à un utilisateur mal intentionné d'obtenir les droits de l'administrateur (root) à distance ;
- libc : un débordement de mémoire lié à l'utilisation des variables d'environnement LANG et LOCPATH permet à un utilisateur local mal intentionné d'obtenir les droits de l'administrateur (root) ;

- NIS : l'arrêt du processus ypbind est possible sous certaines conditions, entraînant ainsi un déni de service ;
- NFS : une attaque par déni de service est possible en inondant le service portmap.

4 Solution

Installer les correctifs mentionnés dans l'avis de Sécurité SSRT-541 (cf. section Documentation).

5 Documentation

Avis de sécurité SSRT-541 de Compaq disponible à l'adresse suivante :
<http://ftp.support.compaq.com/patches/.new/html/SSRT-541.shtml>

Gestion détaillée du document

17 avril 2002 version initiale.