



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 19 juillet 2002
N° CERTA-2002-AVI-152

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités sur HP Compaq Tru64 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-152>

Gestion du document

Référence	CERTA-2002-AVI-152
Titre	Vulnérabilités sur HP Compaq Tru64 Unix
Date de la première version	19 juillet 2002
Date de la dernière version	–
Source(s)	Avis de sécurité SSRT0794U et SSRT0795U de HP
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 ;
- élévation de privilèges ;
- exécution de code arbitraire.

2 Systèmes affectés

- HP Compaq Tru64 Unix version 5.1a ;
- HP Compaq Tru64 Unix version 5.1 ;
- HP Compaq Tru64 Unix version 5.0a ;
- HP Compaq Tru64 Unix version 4.0g ;
- HP Compaq Tru64 Unix version 4.0f.

3 Résumé

Deux vulnérabilités présentes sur HP Compaq Tru64 Unix permettent à un utilisateur mal intentionné de réaliser un déni de service des processus créés par le daemon `inetd` ou d'exécuter du code arbitraire sur la machine avec une élévation des privilèges.

4 Description

Un utilisateur mal intentionné peut, par l'envoi massif de paquets spécifiques, réaliser un déni de service des processus créés par le daemon `inetd` sur les systèmes HP Compaq Tru64 Unix versions 5 énumérés ci-dessus.

La seconde vulnérabilité concerne la commande `ipcs` (Inter-Process Communication Status) utilisée pour visualiser les ressources partagées sur les systèmes Unix. Un utilisateur local mal intentionné peut, en utilisant un débordement de mémoire présent sur cette commande, élever ses privilèges et exécuter du code arbitraire.

5 Solution

Appliquer les correctifs disponibles correspondant à la version de votre système (cf avis de sécurité HP Compaq, section documentation).

6 Documentation

- Avis de sécurité SSRT0794U de HP Compaq :
<http://ftp.support.compaq.com/patches/public/unix/v5.1a/t64v51ab2-c0015807-14563-es-20020611.README>
- Avis de sécurité SSRT0795U de HP Compaq :
<http://ftp.support.compaq.com/patches/public/unix/v5.1a/t64v51ab2-c0035101-14695-es-20020624.README>

Gestion détaillée du document

19 juillet 2002 version initiale.