Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 09 mars 2001
N° CERTA-2001-AVI-031

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de HP OpenView OmniBack sous HP-UX et Windows NT/2000

Gestion du document

Référence	CERTA-2001-AVI-031
Titre	Vulnérabilité de HP OpenView OmniBack sous HP-UX et Windows NT/2000
Date de la première version	09 mars 2001
Date de la dernière version	–
Source(s)	Avis HP #0142
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

Accès complet au système à distance sans compte utilisateur.

2 Systèmes affectés

Windows NT 4.0, Windows 2000 et tous les systèmes HP-UX avec OpenView OmniBack (versions 3.00 et supérieures).

3 Résumé

Un utilisateur mal intentionné peut ouvrir une console avec des droits d'administrateur sur un système ayant le client OpenView Omniback.

4 Description

Le client OpenView Omniback d'HP permet d'effectuer des sauvegardes par le réseau. Une vulnérabilité de ce client permet à un utilisateur d'ouvrir une console à distance avec des droits d'administrateur.

5 Solution

Appliquer le correctif de HP selon la version d'OmniBack et le systèmes d'exploitation, à l'adresse : http://europe-support.external.hp.com

- OmniBack 3.50 sur HP-UX 10.x : PHSS_22914
- OmniBack 3.50 sur HP-UX 11.x : PHSS_22915
- OmniBack 3.10 sur HP-UX 10.x : PHSS_23095
- OmniBack 3.10 sur HP-UX 11.x : PHSS_23096
- OmniBack 3.00 sur HP-UX 10.x : PHSS_23103
- OmniBack 3.00 sur HP-UX 11.x : PHSS_23104

Pour Windows NT et Windows 2000, appliquer le correctif : OmniBack_00017 - OmniBack 3.50

6 Documentation

Bulletin de sécurité de HP #0142 du 28 février 2001 :
http://itrc.hp.com

Gestion détaillée du document

09 mars 2001 version initiale.