



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 28 septembre 2000  
N° CERTA-2000-AVI-053

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans HP OpenView

---

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-2000-AVI-053>

---

### Gestion du document

Référence	CERTA-2000-AVI-053
Titre	Vulnérabilité dans HP OpenView
Date de la première version	28 septembre 2000
Date de la dernière version	–
Source(s)	NTBugTraq
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 ;
- Exécution de code arbitraire.

## 2 Systèmes affectés

- HP Openview Node Manager v6.1 sous HP-UX 11.00 ;
- HP Openview Node Manager v6.1 sous HP-UX 10.X ;
- HP Openview Node Manager v6.1 sous SOLARIS 2.X ;
- HP Openview Node Manager v6.1 sous Windows NT4/2000.

## 3 Résumé

Une vulnérabilité à été découverte dans le service d'alarme de HP Openview Node Manager v6.1.

## 4 Description

HP Openview Node Manager v6.1 possède un service d'alarme ( OVALARMSRV ) qui ne vérifie pas correctement certaines variables d'environnement. Un utilisateur distant, mal intentionné, peut provoquer un débordement de pile créant ainsi un déni de service sur ce service.

## 5 Solution

Correctifs à appliquer suivant les versions d'OS :

- Sous HP-UX 11.00 : PHSS\_22407
- Sous HP-UX 10.X : PHSS\_22406
- Sous SOLARIS 2.X : PSOV\_02830
- Sous Windows NT4/2000 : NNM\_00621

Ces correctifs sont téléchargeables à l'adresse :  
<http://ovweb.external.hp.com/cpe/patches/>

## 6 Documentation

Site HP :  
<http://itrc.hp.com>

## Gestion détaillée du document

28 septembre 2000 version initiale.