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 août 2001
N° CERTA-2001-AVI-087

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de HP Openview NNM

Gestion du document

Référence	CERTA-2001-AVI-087
Titre	Vulnérabilité de HP Openview NNM
Date de la première version	28 août 2001
Date de la dernière version	–
Source(s)	Avis du CERT/CC CA-2001-24 Avis du CIAC L-102 Bulletin de sécurité 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

Exécution de code arbitraire avec des privilèges élevés.

2 Systèmes affectés

Vulnérabilité indépendante de la plate-forme.

3 Résumé

Un utilisateur mal intentionné peut exécuter du code arbitraire avec les privilèges du *daemon* `ovactiond`.

4 Description

`ovactiond` est un élément de HP Openview et Tivoli Netview

Une vulnérabilité de ces logiciels permet à un utilisateur mal intentionné d'accéder à distance aux privilèges de `ovactiond` au moyen d'une commande SNMP particulière.

Pour HP Openview la configuration par défaut permet l'exploitation de cette vulnérabilité. En ce qui concerne Tivoli Netview, une modification de la configuration peut rendre le système vulnérable.

Sous Unix, il s'agit le plus souvent des privilèges de `bin`. Sous Windows NT, `LocalSystem`.

5 Solution

Appliquer le correctif selon le système sur lequel est installé `ovactiond`.

- Pour HP-UX 11.00 : télécharger PHSS_23780.
- Pour HP-UX 10.20 : télécharger PHSS_23779.
- Pour Solaris 2.x : télécharger PSOV_02905.
- Pour Windows NT4 ou 2000 : télécharger le correctif NNM_00698.

Sur le site de HP :
http://ovweb.external.hp.com/cpe/patches/

6 Documentation

- Avis de sécurité HP :
  http://www.itresourcecenter.hp.com/
- Avis de sécurité du CERT/CC :
  http://www.cert.org/advisories/CA-2001-24.html
- Avis de sécurité du CIAC :
  http://www.ciac.org/ciac/bulletins/l-102.shtml

Gestion détaillée du document

28 août 2001 version initiale.