Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 21 février 2002
N° CERTA-2002-AVI-038

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité des agents SNMP pour les équipements HP

Gestion du document

Référence	CERTA-2002-AVI-038
Titre	Vulnérabilité des agents SNMP pour les équipements HP
Date de la première version	21 février 2002
Date de la dernière version	–
Source(s)	Bulletin de sécurité HPSBUX0202-184 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 ;
- accès non autorisé.

2 Systèmes affectés

- Les anciennes versions des produits JetDirect (se référer au bulletin de sécurité HP pour connaître les versions vulnérables) ;
- les commutateurs HP procurve 2524 (Produit J4813A) ;
- *Network Node Manager* (NNM) ;
- HP-UX 10.x 11.x avec `snmpd` ou HPOpenview.

3 Description

Les tests effectués par l'université finlandaise d'Oulu ont mis en évidence la présence de vulnérabilités dans les routines de décodage et de traitement des messages SNMP dans de nombreuses implémentations (se référer au bulletin d'alerte CERTA-2002-ALE-004 du CERTA).

Un utilisateur mal intentionné peut utiliser une vulnérabilité de l'agent SNMP pour exécuter du code arbitraire avec les privilèges de l'administrateur `root` ou effectuer des dénis de services sur les équipements HP concernés.

Cette vulnérabilité, de type débordement de mémoire, est exploitable à distance.

4 Contournement provisoire

- Filtrer le port 161/udp sur le garde-barrière de façon à éviter une attaque provenant de lInternet.
- Pour les systèmes munis de NNM désactiver `snmpd` et `snmpdm`.

NOTA : Dans son bulletin de sécurité, HP souligne le fait que supprimer `snmp` peut entrainer des dysfonctionnements inattendus, entre autres, sur les systèmes EMS (*Event Monitoring System*) et MC/ServiceGuard (supervision des clusters).

5 Solution

Se référer au bulletin de sécurité de HP (cf. section Documentation) pour la disponibilité des correctifs.

6 Documentation

Le bulletin de sécurité HPSBUX0202-184 de HP disponible sur le site :
http://www.itrc.hp.com

Gestion détaillée du document

21 février 2002 version initiale.