

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilités dans HP OpenView NNM

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-2008-ALE-006>

Gestion du document

Référence	CERTA-2008-ALE-006-001
Titre	Vulnérabilités dans HP OpenView NNM
Date de la première version	18 avril 2008
Date de la dernière version	10 juin 2010
Source(s)	CVE-2008-0068, 1697, 1842, 1851, 1852 et 1853
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 à distance ;
- déni de service à distance ;
- contournement de la politique de sécurité.

2 Systèmes affectés

HP OpenView Network Node Manager, version 7.x.
D'autres versions peuvent être affectées.

3 Résumé

Plusieurs vulnérabilités dans HP OpenView Network Node Manager permettent à un utilisateur malveillant de provoquer un déni de service à distance, d'exécuter du code arbitraire à distance ou de contourner la politique de sécurité. Les vulnérabilités ont été corrigées en 2008 et 2009.

4 Description

Plusieurs vulnérabilités sont présentes dans HP OpenView Network Node Manager :

- une vulnérabilité (CVE-2008-0068) provient d'un filtrage insuffisant d'un paramètre de CGI. Son exploitation permet à un utilisateur malveillant de contourner la politique de sécurité ;
- une vulnérabilité (CVE-2008-1697) concerne l'utilisation d'un paramètre de longueur élevée dans une requête HTTP. Cette exploitation permet à un utilisateur malveillant d'exécuter du code arbitraire à distance ;
- une vulnérabilité (CVE-2008-1842) est présente dans le traitement de certaines requêtes vers le port TCP 8886. Son exploitation permet à un utilisateur malveillant de provoquer un déni de service à distance ou d'exécuter du code arbitraire à distance ;
- une vulnérabilité (CVE-2008-1851) provient de l'attente sans limite de temps lorsqu'une requête, adressée au port TCP 2954, est incomplète. Cette vulnérabilité peut servir à réaliser un déni de service ;
- une vulnérabilité (CVE-2008-1852) provient d'un problème d'allocation mémoire, provoqué par la déclaration d'un nombre trop important de paramètres dans une requête adressée au port TCP 2954. L'exploitation de la vulnérabilité provoque un arrêt inopiné du programme ;
- une vulnérabilité (CVE-2008-1853) permet l'arrêt du service par l'envoi d'un paquet d'une certaine forme sur le port TCP 2532. L'utilisateur malveillant peut provoquer un déni de service à distance.

Des codes exploitant ces vulnérabilités sont disponibles sur l'Internet.

5 Contournement provisoire

Dans l'attente d'un correctif, des mesures permettent de limiter la capacité d'exploitation de ces vulnérabilités ou de détecter une telle exploitation :

- n'autoriser l'accès au serveur qu'aux utilisateurs en ayant besoin ;
- filtrer les accès depuis les réseaux vers le serveur HP OpenView Network Node Manager;
- bloquer les flux depuis l'Internet vers le serveur sur les ports TCP 80, 2532, 2954 et 8886 ou vérifier que ce blocage est effectif s'il est déjà prévu dans la politique de sécurité ;
- surveiller attentivement les journaux des filtres et des serveurs, en particulier l'activité liée à ces ports et l'activité depuis le serveur HP OpenView Network Node Manager.

6 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

7 Documentation

- Site de téléchargement des correctifs HP :
<http://support.openview.hp.com/selfsolve/patches>
- Bulletin de sécurité HP c01471755 du 10 juin 2008 :
<http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01471755>
- Bulletin de sécurité HP c01495949 du 11 mai 2009 :
<http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01495949>
- Bulletin de sécurité HP c01496048 du 11 mai 2009 :
<http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01496048>
- Référence CVE CVE-2008-0068 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0068>
- Référence CVE CVE-2008-1697 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1697>
- Référence CVE CVE-2008-1842 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1842>
- Référence CVE CVE-2008-1851 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1851>

- Référence CVE CVE-2008-1852 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1852>
- Référence CVE CVE-2008-1853 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1853>

Gestion détaillée du document

18 avril 2008 version initiale.

10 juin 2010 ajout des correctifs et des bulletins HP.