

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités 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-2008-AVI-214>

Gestion du document

Référence	CERTA-2008-AVI-214
Titre	Multiples vulnérabilités dans HP Openview
Date de la première version	17 avril 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité HP HPSBMA02328 du 15 avril 2008
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 (NNM) 6.41 ;
- HP Openview Network Node Manager (NNM) 7.01 ;
- HP Openview Network Node Manager (NNM) 7.51.

3 Résumé

De multiples vulnérabilités permettant l'exécution de code arbitraire depuis un réseau local ont été corrigées dans HP Openview.

4 Description

HP Openview a publié le 15 avril 2008 un correctif de sécurité permettant de résoudre plusieurs anciennes vulnérabilités présentes au niveau de la version embarquée d'Apache.

Ces vulnérabilités permettent à un utilisateur malintentionné de réaliser de l'injection de code indirecte (XSS), un déni de service à distance depuis le réseau local, ou l'exécution de code arbitraire à distance depuis le réseau local.

5 Solution

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

6 Documentation

- Bulletin de sécurité HP HPSBMA02328 du 15 avril 2008 :
<http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01428449>
- Référence CVE CVE-2005-3352 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-3352>
- Référence CVE CVE-2005-3357 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-3357>
- Référence CVE CVE-2006-3747 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3747>

Gestion détaillée du document

17 avril 2008 version initiale.