

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : 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-2005-AVI-379>

Gestion du document

Référence	CERTA-2005-AVI-379
Titre	Vulnérabilités dans HP OpenView
Date de la première version	05 octobre 2005
Date de la dernière version	–
Source(s)	Bulletins de sécurité SSRT051030 et SSRT051023 du 03 octobre 2005
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.

2 Systèmes affectés

- HP OpenView Network Node Manager (OV NNM) versions 6.20, 6.4x, 7.01 et 7.50 ;
- HP OpenView Event Correlation Services (OV ECS) versions 3.10, 3.20, 3.30, 3.31, 3.32 et 3.33.

3 Résumé

Deux vulnérabilités dans HP OpenView Event Correlation Services et dans HP OpenView Network Node Manager permettent l'exécution de code arbitraire à distance.

4 Description

Des vulnérabilités ont été découvertes dans les fichiers :

- `connectedNodes.ovpl` de HP OpenView Network Node Manager ;

- ecscmg.ovpl de HP OpenView Event Correlation Services.

L'exploitation de ces vulnérabilités permet l'exécution de code arbitraire à distance.

Du code malveillant permettant d'exploiter la vulnérabilité d'OpenView Network Node Manager est disponible sur l'Internet.

5 Contournement provisoire

Filtrer le port 3443/tcp (vulnérabilité d'OpenView Network Node Manager).

6 Solution

Appliquer les correctifs de l'éditeur (voir section Documentation).

7 Documentation

- Site Internet de l'éditeur :
<http://support.openview.hp.com>
- Bulletin de sécurité SSRT051023 du 03 octobre 2005 :
http://support.openview.hp.com/news.jsp#nnm_security
- Bulletin de sécurité SSRT051030 du 03 octobre 2005 :
<http://support.openview.hp.com/news.jsp#ecs>

Gestion détaillée du document

05 octobre 2005 version initiale.