



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 10 août 2007
N° CERTA-2007-AVI-351

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-2007-AVI-351>

Gestion du document

Référence	CERTA-2007-AVI-351
Titre	Multiples vulnérabilités dans HP OpenView
Date de la première version	10 août 2007
Date de la dernière version	–
Source(s)	Bulletins de sécurité HP HPSBMA02235 à HPSBMA002246 du 07 août 2007
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.

2 Systèmes affectés

- HP Business Process Insight (HPBPI) 1.x ;
- HP Business Process Insight (HPBPI) 2.x ;
- HP OpenView Business Process Insight (OVBPI) 1.x ;
- HP OpenView Business Process Insight (OVBPI) 2.x ;
- HP OpenView Dashboard 2.x ;
- HP OpenView Internet Service (OVIS) 6.x ;
- HP OpenView Network Node Manager (NNM) 6.x ;
- HP OpenView Network Node Manager (NNM) 7.x ;
- HP OpenView Operations HTTPS Agent 8.x ;
- HP OpenView Operations Manager for Windows (OVOW) 7.x ;
- HP OpenView Performance Agent ;
- HP OpenView Performance Insight (OVPI) 5.x ;

- HP OpenView Performance Manager (OVPM) 5.x ;
- HP OpenView Performance Manager (OVPM) 6.x ;
- HP OpenView Reporter 3.x ;
- HP OpenView Service Desk Process Insight (SDPI) 1.x ;
- HP OpenView Service Desk Process Insight (SDPI) 2.x ;
- HP OpenView Service Quality Manager (OV SQM) 1.x ;
- HP Service Desk Process Insight (HPSDPI) 1.x ;
- HP Service Desk Process Insight (HPSDPI) 2.x.

3 Résumé

Plusieurs applications de HP OpenView sont vulnérables à un débordement de mémoire.

4 Description

Un service partagé par plusieurs applications est vulnérable à un débordement de mémoire, ce qui rend les logiciels l'utilisant vulnérables. Un utilisateur malintentionné pourrait exploiter ces failles pour exécuter du code arbitraire à distance.

5 Solution

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

6 Documentation

- Bulletins de sécurité HPSBMA02235 à HPSBMA002246 du 07 août 2007 :
<http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01106515>
<http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01109171>
<http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01109584>
<http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01109617>
<http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01110576>
<http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01110627>
<http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01111851>
<http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01112038>
<http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01114023>
<http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01114156>
<http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01115068>
- Référence CVE CVE2007-3872:
<http://cve.mitre.org/cgi-bin/cvename.cgi.name=CVE-2007-3872>

Gestion détaillée du document

10 août 2007 version initiale.