



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 14 avril 2011
N° CERTA-2011-AVI-219

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans HP Network Node Manager i

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-2011-AVI-219>

Gestion du document

Référence	CERTA-2011-AVI-219
Titre	Vulnérabilités dans HP Network Node Manager i
Date de la première version	14 avril 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité HP c02746026 et c02729035 du 12 avril 2011
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 distant ;
- contournement de la politique de sécurité ;
- injection de code indirecte à distance.

2 Systèmes affectés

HP Network Node Manager i 8.1x et 9.0x

3 Résumé

Plusieurs vulnérabilités ont été découvertes dans *HP Network Node Manager i* permettant un déni de service, un contournement de la politique de sécurité et une injection indirecte de code à distance.

4 Description

Trois vulnérabilités ont été découvertes dans *HP Network Node Manager i*. La première (CVE-2010-4476) permet à un utilisateur malveillant d'effectuer un déni de service à distance. Elle provient de l'environnement

d'exécution Java inclus dans les versions 8.1x et 9.0x de *HP Network Node Manager i* qui ne gère pas correctement certaines conversions de nombres flottants. Les deux autres vulnérabilités n'affectent que les versions 9.0x de *HP Network Node Manager i*. La première (CVE-2011-0897) permet à un utilisateur local malintentionné d'obtenir un accès non autorisé à des fichiers. La seconde (CVE-2011-0898) autorise un utilisateur distant à injecter indirectement du code.

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 c02746026 du 12 avril 2011 :
<http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02746026>
- Bulletin de sécurité HP c02729035 du 12 avril 2011 :
<http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02729035>
- Référence CVE CVE-2010-4476 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-4476>
- Référence CVE CVE-2011-0897 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0897>
- Référence CVE CVE-2010-0898 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0898>

Gestion détaillée du document

14 avril 2011 version initiale.