

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans JP1/Cm2/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-2012-AVI-104>

Gestion du document

Référence	CERTA-2012-AVI-104
Titre	Multiples vulnérabilités dans JP1/Cm2/Network Node Manager i
Date de la première version	01 mars 2012
Date de la dernière version	–
Source(s)	Bulletin de sécurité Hitachi HS12-009 du 29 février 2012
Pièce(s) jointe(s)	Aucune

TAB. 1 – Gestion du document

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risques

- Exécution de code arbitraire à distance ;
- déni de service à distance.

2 Systèmes affectés

- JP1/Cm2/Network Node Manager i versions 09-00 à 09-00-05, 09-10 à 09-10-03 et 09-50 à 09-50-02 ;
- JP1/Cm2/Network Node Manager i Advanced versions 09-10 à 09-10-03 et 09-50 à 09-50-02.

3 Résumé

De multiples vulnérabilités dans JP1/Cm2/Network Node Manager i permettent de réaliser un déni de service et d'exécuter du code arbitraire à distance.

4 Description

De multiples vulnérabilités ont été découvertes dans JP1/Cm2/Network Node Manager i. L'exploitation de celles-ci permet de réaliser un déni de service et d'exécuter du code arbitraire à distance.

5 Solution

Les vulnérabilités sont corrigées dans la version 09-50-03 du 29 février 2012 de *JPI/Cm2/Network Node Manager i*.

6 Documentation

- Bulletin de sécurité Hitachi HS12-009 du 29 février 2012 :
<http://www.hitachi.co.jp/Prod/comp/soft1/global/security/info/vuls/HS12-009/index.html>

Gestion détaillée du document

01 mars 2012 version initiale.