

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans Hitachi JP1

---

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-617>

---

### Gestion du document

Référence	CERTA-2012-AVI-617
Titre	Multiples vulnérabilités dans Hitachi JP1
Date de la première version	02 novembre 2012
Date de la dernière version	–
Source(s)	Bulletin de sécurité HS12-022 du 01 novembre 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 Risque

- Exécution de code arbitraire à distance ;
- contournement de la politique de sécurité ;
- atteinte à la confidentialité des données.

## 2 Systèmes affectés

Hitachi JP1/File Transmission Server/FTP versions antérieures à 10-00.

## 3 Résumé

Trois vulnérabilités ont été corrigées dans *Hitachi JP1/File Transmission Server/FTP*. La première concerne le mode PASV qui peut permettre à un attaquant de scanner des ports au moyen du serveur. La deuxième provoque un débordement de mémoire tampon lors de la transmission d'un fichier. La troisième affecte le système de validation des comptes utilisateurs lors de leurs authentications.

## 4 Solution

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

## **5 Documentation**

- Bulletin de sécurité HS12-022 du 01 novembre 2012 :  
<http://www.hitachi.co.jp/Prod/comp/soft1/security/info/vuls/HS12-022/index.html>

### **Gestion détaillée du document**

**02 novembre 2012** version initiale.