

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans Novell iChain FTP Server

---

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-109>

---

### Gestion du document

Référence	CERTA-2005-AVI-109
Titre	Multiples vulnérabilités dans Novell iChain FTP Server
Date de la première version	14 mars 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité Novell 10096885 du 11 mars 2005 Bulletin de sécurité Novell 10096886 du 11 mars 2005
Pièce(s) jointe(s)	

TAB. 1 – Gestion du document

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

## 1 Risque

- Atteinte à la confidentialité des données ;
- contournement de la politique de sécurité.

## 2 Systèmes affectés

iChain 2.x.

## 3 Résumé

Deux vulnérabilités découvertes dans iChain permettent à un utilisateur mal intentionné de porter atteinte à la confidentialité des données ou de contourner la politique de sécurité du système vulnérable.

## 4 Description

Novell iChain est outil permettant la gestion des identités.

- Une vulnérabilité découverte dans le GUI (Graphic User Interface) permet à un utilisateur mal intentionné présent sur le réseau local et analysant le trafic réseau d’avoir un accès non autorisé à la session administrateur et de pouvoir administrer le serveur iChain;
- la seconde vulnérabilité permet à un individu distant mal intentionné de porter atteinte à la confidentialité des données, au moyen de la commande `pwd` qui est tolérée par le serveur iChain.

## **5 Contournement provisoire**

L’éditeur recommande de :

- limiter l’accès au serveur iChain via le port 51100/tcp ;
- limiter l’accès au serveur FTP.

## **6 Solution**

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

## **7 Documentation**

- Bulletin de sécurité Novell 10096885 du 11 mars 2005 :  
<http://support.novell.com/cgi-bin/search/searchtid.cgi?/10096885.htm>
- Bulletin de sécurité Novell 10096886 du 11 mars 2005 :  
<http://support.novell.com/cgi-bin/search/searchtid.cgi?/10096886.htm>

## **Gestion détaillée du document**

**14 mars 2005** version initiale.