



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 06 décembre 2007  
N° CERTA-2007-AVI-526

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans Novell BorderManager

---

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-526>

---

### Gestion du document

Référence	CERTA-2007-AVI-526
Titre	Vulnérabilités dans Novell BorderManager
Date de la première version	06 décembre 2007
Date de la dernière version	–
Source(s)	
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.

## 2 Systèmes affectés

Novell BorderManager 3.X.

## 3 Résumé

Deux vulnérabilités découvertes dans Novell BorderManager permettent à un utilisateur distant malintentionné de contourner la politique de sécurité ou d'exécuter du code arbitraire à distance.

## 4 Description

L'une des vulnérabilités est causée par une erreur dans le traitement des requêtes UDP vers le service Client Trust Application. Cette vulnérabilité, de type débordement de mémoire, affecte le fichier `clntrust.exe` et peut être exploitée par une personne malveillante afin d'exécuter du code arbitraire à distance.

L'autre vulnérabilité est causée par une erreur dans le traitement du trafic HTTP encodé en unicode qui permet à une personne malintentionnée de contourner la politique de sécurité.

## **5 Solution**

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

## **6 Documentation**

- Bulletin de sécurité Novell #5007301 du 04 décembre 2007 :  
[http://support.novell.com/docs/Readmes/InfoDocument/patchbuilder/readme\\_5007301.html](http://support.novell.com/docs/Readmes/InfoDocument/patchbuilder/readme_5007301.html)
- Référence CVE CVE-2007-5767 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5767>

## **Gestion détaillée du document**

**06 décembre 2007** version initiale.