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 novembre 2006
N° CERTA-2006-AVI-494

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Novell BorderManager

Gestion du document

Référence	CERTA-2006-AVI-494
Titre	Vulnérabilité de Novell BorderManager
Date de la première version	14 novembre 2006
Date de la dernière version	–
Source(s)	Document 3003139 de Novell du 10 novembre 2006
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 à distance ;
- contournement de la politique de sécurité ;
- atteinte à l'intégrité des données ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

- Novell BoarderManager 3.8, avec le Support Pack 4, ainsi que les versions antérieures.

3 Description

Une vulnérabilité a été identifiée dans le produit Novell BoarderManager 3.8. Il semblerait que les fichiers de sessions ISAKMP (ou *cookies*) ne soient pas générés correctement à chaque nouvelle session. Une personne se connectant (avec une adresse source IP et un port donné), risque de garder les mêmes fichiers de sessions pour toutes les requêtes dans une période de plusieurs heures, ce qui les rend prévisibles.

Une personne malveillante qui récupérerait de tels fichiers pourrait contourner la politique de sécurité imposée par IPsec, afin de lancer un déni de service contre le système BoarderManager vulnérable, voire lancer des attaques en réinjectant tout ou partie des paquets interceptés.

4 Solution

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

5 Documentation

– Document 3003139 de Novell du 10 novembre 2006 :
https://secure-support.novell.com/KanisaPlatform/Publishing/201/3003139_f.SAL_Public.html

Gestion détaillée du document

14 novembre 2006 version initiale.