



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 19 janvier 2006  
N° CERTA-2006-AVI-037

Affaire suivie par :  
CERTA

## AVIS DU CERTA

**Objet : Vulnérabilité dans le produit Enterprise Server Remote Manager de Novell**

---

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-2006-AVI-037>

---

### Gestion du document

Référence	CERTA-2006-AVI-037
Titre	Vulnérabilité dans le produit Enterprise Server Remote Manager de Novell
Date de la première version	19 janvier 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité iDefense
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 ;
- déni de service à distance.

## 2 Systèmes affectés

Novell SUSE Linux Open Enterprise Server.

## 3 Résumé

Un utilisateur distant mal intentionné peut envoyer au service une requête HTTP volontairement mal formée qui pourrait permettre l'exécution de code arbitraire.

## 4 Description

Enterprise Server Remote Manager est une solution d'administration à distance utilisant le protocole HTTP. Une faille dans l'interprétation des entêtes HTTP par le service, permet un débordement de tampon dans la pile et donc éventuellement l'exécution de code arbitraire.

## 5 Contournement provisoire

Restreindre l'accès à des adresses IP de confiance à l'aide d'un pare-feu en coupure (ports par défaut 8008/tcp et 8009/tcp).

## 6 Solution

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

## 7 Documentation

- Bulletin de sécurité SUSE SuSE-SA:2006:002 du 13 janvier 2006 :  
[http://www.novell.com/linux/security/advisories/2006\\_02\\_novellnrm.html](http://www.novell.com/linux/security/advisories/2006_02_novellnrm.html)
- Bulletin de sécurité iDefense du 13 janvier 2006 :  
<http://www.odefense.com/application/poi/display?id=371>
- Référence CVE CAN-2005-3655 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-3655>

## Gestion détaillée du document

**19 janvier 2006** version initiale.