

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans Novell eDirectory

---

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-2008-AVI-532>

---

### Gestion du document

Référence	CERTA-2008-AVI-532
Titre	Multiples vulnérabilités dans Novell eDirectory
Date de la première version	30 octobre 2008
Date de la dernière version	–
Source(s)	Bulletins de sécurité Novell #5037180 et #5037181 du 23 octobre 2008
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

- Injection de code indirecte (XSS) ;
- inconnu.

## 2 Systèmes affectés

- Novell eDirectory 8.x.

## 3 Résumé

Plusieurs vulnérabilités ont été découvertes dans Novell eDirectory permettant, entre autres, une injection de code indirecte (XSS).

## 4 Description

Plusieurs vulnérabilités affectent Novell eDirectory :

- de multiples dépassements de tas ont été découverts ;

- une corruption de mémoire à distance est possible via *NCP* ;
- *httpstk* permet d'effectuer une injection de code indirecte.

## 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 #5037180 du 23 octobre 2008 :  
[http://support.novell.com/docs/Readmes/InfoDocument/patchbuilder/readme\\_5037180.html](http://support.novell.com/docs/Readmes/InfoDocument/patchbuilder/readme_5037180.html)
- Bulletin de sécurité Novell #5037181 du 23 octobre 2008 :  
[http://support.novell.com/docs/Readmes/InfoDocument/patchbuilder/readme\\_5037181.html](http://support.novell.com/docs/Readmes/InfoDocument/patchbuilder/readme_5037181.html)
- Référence CVE CVE-2008-0925 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0925>
- Référence CVE CVE-2008-4478 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4478>
- Référence CVE CVE-2008-4479 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4479>
- Référence CVE CVE-2008-4480 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4480>

## Gestion détaillée du document

**30 octobre 2008** version initiale.