Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 20 juin 2008
N° CERTA-2008-AVI-330

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Novell eDirectory

Gestion du document

Référence	CERTA-2008-AVI-330
Titre	Vulnérabilité de Novell eDirectory
Date de la première version	20 juin 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité Novell 3460217
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

Contournement de la politique de sécurité.

2 Systèmes affectés

- Novell eDirectory 8.8.2 et versions antérieures pour Solaris ;
- Novell eDirectory 8.8.2 et versions antérieures pour Linux ;
- Novell eDirectory 8.8.2 et versions antérieures pour Windows 2003 ;
- Novell eDirectory 8.8.2 et versions antérieures pour Windows 2000 ;
- Novell eDirectory 8.7.3.9 et versions antérieures pour Solaris ;
- Novell eDirectory 8.7.3.9 et versions antérieures pour Linux ;
- Novell eDirectory 8.7.3.9 et versions antérieures pour Windows 2003 ;
- Novell eDirectory 8.7.3.9 et versions antérieures pour Windows 2000 ;

3 Résumé

Une vulnérabilité a été découverte dans `Novell eDirectory`. L'exploitation de celle-ci conduit à une attaque par injection de code indirecte (*Cross Site Scripting*).

4 Description

Une vulnérabilité a été découverte dans l'interface *iMonitor* de `Novell eDirectory`. Cette interface ne gère pas correctement le retour de certains pages et permet ainsi d'effectuer des attaques par injection de code indirecte (*Cross Site Scripting*).

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 3460217 :
  http://www.novell.com/support/viewContent.do?externalId=3460217&sliceId=1
- Référence CVE CVE-2008-0925 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0925

Gestion détaillée du document

20 juin 2008 version initiale.