Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 24 octobre 2006
N° CERTA-2006-AVI-462

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Novell eDirectory

Gestion du document

Référence	CERTA-2006-AVI-462
Titre	Multiples vulnérabilités dans Novell eDirectory
Date de la première version	24 octobre 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité de Novell eDirectory
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 eDirectory versions antérieures à 8.8.1.

3 Résumé

De multiples vulnérabilités présentes dans Novell eDirectory permettent à un utilisateur mal intentionné d'exécuter du code arbitraire à distance ou de réaliser un déni de service.

4 Description

NCP (NetWare Core Protocol) est le principal protocole utilisé par Novell pour la transmission d'information entre le serveur NetWare et ses clients.
Deux vulnérabilités de type dépassement de mémoire existent dans le protocole NCP permettant à un utilisateur

distant mal intentionné de réaliser un deni de service, d'exécuter du code arbitraire ou de faire anormalement grossir les journaux d'événements de `Novell eDirectory`.
Deux autres vulnérabilités existent dans la fonction `evtFilteredMonitorEventsRequest` dues à une mauvaise gestion de l'allocation et de la libération de la mémoire. Ces vulnérabilités permettent à un utilisateur mal intentionné de réaliser un déni de service ou d'exécuter du code arbitraire à distance.

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 TID 3924657 du 23 octobre 2006 :
  http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=3924657&sliceID=SAL_Public&dialo
- Bulletin de sécurité Novell TID 3686202 du 23 octobre 2006 :
  http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=3686202&sliceID=SAL_Public&dialo
- Bulletin de sécurité Novell TID 3936018 du 23 octobre 2006 :
  http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=3936018&sliceID=SAL_Public&dialo
- Bulletin de sécurité Novell TID 3496175 du 23 octobre 2006 :
  http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=3496175&sliceID=SAL_Public&dialo
- Référence CVE CVE-2006-4509 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4509
- Référence CVE CVE-2006-4510 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4510
- Référence CVE CVE-2006-4520 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4520
- Référence CVE CVE-2006-4177 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4177

Gestion détaillée du document

24 octobre 2006 version initiale.