Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 06 février 2008
N° CERTA-2008-AVI-052

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans des produits Novell

Gestion du document

Référence	CERTA-2008-AVI-052
Titre	Vulnérabilités dans des produits Novell
Date de la première version	06 février 2008
Date de la dernière version	–
Source(s)	Avis de mises à jour Novell 3908994 et 3726376 du 04/05 février 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

- Contournement de la politique de sécurité ;
- atteinte à l'intégrité des données ;
- atteinte à la confidentialité des données ;
- élévation de privilèges.

2 Systèmes affectés

- Novell ZENworks Patch Management 6.2 : ZPM Update Agent pour la version 6.2094 ou celles antérieures ;
- Novell ZENworks Patch Management 6.3 : ZPM Update Agent pour la version 6.3450 ou celles antérieures ;
- Novell ZENworks Patch Management 6.4 : ZPM Update Agent pour la version 6.4102 ou celles antérieures ;
- Novell Challenge Response Client (LCM) version 2.7.5 ainsi que celles antérieures. Cette version est fournie avec Novell Client 4.91 SP4 dans le produit NMAS (Novell Modular Authentication Services).

3 Résumé

Des vulnérabilités ont été identifiées dans des produits Novell. Elles permettraient à des utilisateux malveillants locaux d'élever leur privilège, d'accéder à des informations sensibles ou à modifier illégitimement des données.

4 Description

Des vulnérabilités ont été identifiées dans des produits Novell :

1. deux vulnérabilités dans Novell ZENworks Patch Management permettent à un utilisateur malveillant local de modifier des fichiers arbitraires ou d'élever ses privilèges. Elles concernent le script `logtrimmer` et la fonction `rebootTask`.
2. une vulnérabilité a été identifiée dans Novell Challenge Response Client. Elle permettrait à des utilisateurs locaux d'accéder à des informations sensibles.

5 Solution

Se référer aux bulletins de sécurité de Novell pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Référence CVE CVE-2008-0525 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0525
- Document Novell de référence 3908994 publié le 05 février 2008 :
  https://secure-support.novell.com/KanisaPlatform/Publishing/18/3908994_f.SAL_Public.html
- Document Novell de référence 3726376 publié le 04 février 2008 :
  https://secure-support.novell.com/KanisaPlatform/Publishing/686/3726376_f.SAL_Public.html

Gestion détaillée du document

06 février 2008 version initiale.