



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 14 novembre 2011  
N° CERTA-2011-AVI-629

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans Novell ZENworks

---

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-2011-AVI-629>

---

### Gestion du document

Référence	CERTA-2011-AVI-629
Titre	Vulnérabilités dans Novell ZENworks
Date de la première version	14 novembre 2011
Date de la dernière version	–
Source	Bulletin de sécurité Novell 7009570 du 19 octobre 2011
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.

## 2 Systèmes affectés

- Novell ZENworks 10 Configuration Management avec SP2 ou SP3 ;
- Novell ZENworks 11 Configuration Management avec SP1 ;
- Novell ZENworks AdminStudio.

## 3 Résumé

Des vulnérabilités dans les produits Novell ZENworks permettent à un utilisateur malintentionné d'exécuter du code arbitraire.

## 4 Description

Des vulnérabilités sont présentes dans les produits Novell ZENworks :

- des vulnérabilités dans *mscomct2.ocx*, appelé directement par ZENworks, déjouant la protection par *killbit* ;

- une absence de filtrage des paramètres transmis à la fonction *LaunchProcess* ;
- un dépassement de tampon mémoire pour le paramètre *bstrReplaceText*.

Toutes ces vulnérabilités permettent à un utilisateur malintentionné d'exécuter du code arbitraire. L'exploitation peut se faire à distance sous réserve d'inciter un utilisateur local à visiter un fichier malveillant distant.

## **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 7009570 du 19 octobre 2011 :  
<http://www.novell.com/support/viewContent.do?externalId=7009570>

## **Gestion détaillée du document**

**14 novembre 2011** version initiale.