

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans LANDesk Management Suite

---

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-2007-AVI-176>

---

### Gestion du document

Référence	CERTA-2007-AVI-176
Titre	Vulnérabilité dans LANDesk Management Suite
Date de la première version	16 avril 2007
Date de la dernière version	–
Source(s)	Base de connaissances LANDesk 4142 du 13 avril 2007
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.

## 2 Systèmes affectés

– LANDesk Management Suite 8.7.

## 3 Description

Une vulnérabilité a été identifiée dans le produit d'administration LANDesk Management Suite. Ce dernier permet de prendre en charge des tâches automatiques de gestion d'un parc de systèmes d'informations.

Il ouvre par défaut un service d'alerte (`aolnsrvr.exe`) en écoute sur le port UDP 65535. Celui-ci ne manipulerait pas correctement les informations reçues, pouvant ainsi conduire à un débordement de tampon.

Une personne malveillante pourrait exploiter cette vulnérabilité pour exécuter du code arbitraire à distance, avec les droits de l'utilisateur SYSTEM.

## 4 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

## 5 Documentation

- Page d'accueil de l'application LANDesk Management Suite :  
<http://www.landesk.fr/Products/LDMS/>
- Base de connaissances LanDesk numéro 4142 publiée le 13 avril 2007 :  
<http://kb.landesk.com/al/12/4/article.asp?aid=4142&n=1&tab=search&bt=4n&s=1>
- Avis de sécurité du groupe de recherche 3Com TippingPoint TSRT-07-04 du 13 avril 2007 :  
<http://www.tippingpoint.com/security/advisories/TSRT-07-04.html>
- Référence CVE CVE-2007-1674 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1674>

### Gestion détaillée du document

16 avril 2007 version initiale.