

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans SNMPc

---

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-2008-AVI-224>

---

### Gestion du document

Référence	CERTA-2008-AVI-224
Titre	Vulnérabilité dans SNMPc
Date de la première version	02 mai 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité Secunia 30036 du 01 mai 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

- Déni de service à distance ;
- exécution de code arbitraire à distance.

## 2 Systèmes affectés

SNMPc version 7.x.

## 3 Résumé

Une vulnérabilité dans *SNMPc* a été découverte permettant à une personne malveillante d'effectuer un déni de service ou une exécution de code arbitraire à distance.

## 4 Description

Une vulnérabilité de *SNMPc* a été découverte dans le traitement des paquets *SNMP TRAP*. L'exploitation de cette vulnérabilité permet à un individu malintentionné d'effectuer un déni de service ou une exécution de code arbitraire à distance.

## **5 Solution**

Se référer au site de l'éditeur pour l'obtention de la mise à jour (cf. section Documentation).

## **6 Documentation**

- Site de *Castlerock* :  
<http://www.castlerock.com/products/snmpc/default.php>
- Alerte de Secunia numéro 30036 du 01 mai 2008 :  
<http://secunia.com/advisories/30036/>

## **Gestion détaillée du document**

**02 mai 2008** version initiale.