

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans IBM Tivoli Netcool Security Manager

---

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-523>

---

### Gestion du document

Référence	CERTA-2007-AVI-523
Titre	Vulnérabilité dans IBM Tivoli Netcool Security Manager
Date de la première version	05 décembre 2007
Date de la dernière version	-
Source(s)	Note d'information d'IBM 24017633 du 30 novembre 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

Contournement de la politique de sécurité.

## 2 Systèmes affectés

- IBM Tivoli Netcool Security Manager version 1.3

## 3 Résumé

Une vulnérabilité de type « injection de code indirecte », ou *cross-site scripting*, a été identifiée dans le produit IBM Tivoli Netcool Security Manager.

## 4 Description

Une vulnérabilité de type « injection de code indirecte », ou *cross-site scripting*, a été identifiée dans le produit IBM Tivoli Netcool Security Manager.

Celle-ci peut être exploitée par une personne malveillante distante pour exécuter du code sur le navigateur d'un utilisateur connecté au service. Ce code aura les mêmes droits contextuels que ceux accordés au site d'IBM

Tivoli Netcool Security Manager. Il est par exemple possible dans ces conditions de dérober les fichiers de session (*cookies*) et lancer des actions sur l'application via le poste de l'utilisateur.

## **5 Solution**

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation). Deux correctifs ont été successivement édités par IBM suite à cette vulnérabilité.

## **6 Documentation**

- Bulletin de sécurité IBM swg24017385 du 01 novembre 2007 :  
<http://www-1.ibm.com/support/docview.wss?uid=swg24017385>
- Bulletin de sécurité IBM swg24017633 du 30 novembre 2007 :  
<http://www-1.ibm.com/support/docview.wss?uid=swg24017633>
- Référence CVE CVE-2007-6219 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6219>

## **Gestion détaillée du document**

**05 décembre 2007** version initiale.