

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité d'ISS Scanner

---

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-2002-AVI-214>

---

### Gestion du document

|                             |                             |
|-----------------------------|-----------------------------|
| Référence                   | CERTA-2002-AVI-214          |
| Titre                       | Vulnérabilité d'ISS Scanner |
| Date de la première version | 19 septembre 2002           |
| Date de la dernière version | –                           |
| Source(s)                   | Alerte ISS                  |
| 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 sur la machine utilisant ISS Scanner.

## 2 Systèmes affectés

Internet Scanner 6.2.1 pour Windows NT et Windows 2000.

## 3 Résumé

Une vulnérabilité dans ISS Scanner permet à un utilisateur mal intentionné, sous certaines conditions, d'exécuter du code arbitraire à distance sur le système utilisant ce scanner.

## 4 Description

ISS Scanner est un scanner de vulnérabilités utilisé généralement pour réaliser un audit de sécurité du réseau. Le fonctionnement d'ISS Scanner repose sur le sondage du réseau et l'interprétation des résultats, notamment des bannières.

Une vulnérabilité d'ISS Scanner dans le traitement des réponses des serveurs Web a été découverte. L'exploitation de cette vulnérabilité par un utilisateur mal intentionné permet l'exécution de code arbitraire à distance sur le système utilisant ISS Scanner.

## **5 Solution**

Appliquer le correctif X-Press Update 6.17 d'ISS :  
<http://www.iss.net/download>

## **6 Documentation**

Alerte d'ISS :  
<http://bvlive01.iss.net/issEn/delivery/xforce/alertdetail.jsp?oid=21165>

## **Gestion détaillée du document**

**19 septembre 2002** version initiale.