



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 02 mai 2002
N° CERTA-2002-AVI-094

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité sur RealSecure Network Sensor

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-094>

Gestion du document

Référence	CERTA-2002-AVI-094
Titre	Vulnérabilité sur RealSecure Network Sensor
Date de la première version	02 mai 2002
Date de la dernière version	–
Source(s)	Liste de diffusion Bugtraq
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.

2 Systèmes affectés

- RealSecure Network Sensor 5.x;
- RealSecure Network Sensor 6.0;
- RealSecure Network Sensor 6.5.

3 Résumé

Un utilisateur mal intentionné peut réaliser un déni de service sur RealSecure Network Sensor de ISS (Internet Security Systems) par le biais de paquets malicieusement construits.

4 Description

RealSecure Network Sensor est un système de détection d'intrusions.

Une vulnérabilité présente dans le traitement de certaines requêtes DHCP peut entraîner l'arrêt intempestif de RealSecure Network Sensor.

Cette vulnérabilité est exploitable à distance.

5 Contournement provisoire

Désactiver les signatures DHCP_ACK, DHCP_Discover et DHCP_Request dans la configuration de RealSecure Network Sensor.

6 Solution

Appliquer la mise à jour RealSecure X-Press Update 4.3 (se référer à la section documentation).

7 Documentation

Site Internet de ISS :

<http://www.iss.net/>

Gestion détaillée du document

02 mai 2002 version initiale.