

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité du logiciel client IVE de Juniper

---

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-2006-AVI-174>

---

### Gestion du document

Référence	CERTA-2006-AVI-174
Titre	Vulnérabilité du logiciel client IVE de Juniper
Date de la première version	27 avril 2006
Date de la dernière version	–
Source(s)	Avis de sécurité Eeye
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 ;
- déni de service à distance.

## 2 Systèmes affectés

IVE OS versions 1.x à 5.x.

## 3 Résumé

Un contrôle *ActiveX* est installé dans le navigateur *Internet Explorer* de toute station cliente ayant réalisé une connexion avec un équipement *IVE* de *Juniper*. Une vulnérabilité dans ce greffon peut être exploitée pour exécuter du code arbitraire avec les privilèges de l'utilisateur du navigateur.

## 4 Description

*IVE* (« Instant Virtual Extranet ») est un système de sécurisation des connexions distantes reposant sur *SSL* ; ceci permet de créer un tunnel en utilisant la couche *SSL* des navigateurs présents sur les stations clientes.

L'utilisation de cette couche nécessite cependant l'utilisation d'un greffon *ActiveX* au sein d'*Internet Explorer* qui est automatiquement téléchargé lors de la connexion à un équipement *IVE*.

Hors ce greffon peut être invoqué par n'importe quelle page *HTML* de n'importe quel site web. A l'aide de paramètres habilement construits, un site malicieux peut alors exploiter la faille du greffon pour faire exécuter du code arbitraire.

## **5 Contournement provisoire**

Désactiver l'utilisation des composants *ActiveX* dans *Internet Explorer*.

## **6 Solution**

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

## **7 Documentation**

- Bulletin de sécurité Juniper du 25 avril 2006 :  
<http://www.juniper.net/support/security/alerts/PSN-2006-03-013.txt>
- Bulletin de sécurité eEye AD20060424 du 25 avril 2006 :  
<http://www.eeye.com/html/research/advisories/AD20060424.html>

## **Gestion détaillée du document**

**27 avril 2006** version initiale.