

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans InterScan Web Security Virtual Appliance

---

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-2010-AVI-286>

---

### Gestion du document

Référence	CERTA-2010-AVI-286
Titre	Vulnérabilités dans InterScan Web Security Virtual Appliance
Date de la première version	23 juin 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité Trend Micro du 14 juin 2010
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 ;
- élévation de privilèges ;
- injection de requêtes illégitimes par rebond.

## 2 Systèmes affectés

*InterScan Web Security Virtual Appliance* version 5.0.

## 3 Résumé

Plusieurs vulnérabilités dans *InterScan Web Security Virtual Appliance* permettent, sous certaines conditions, l'exécution de code arbitraire.

## 4 Description

- Plusieurs vulnérabilités ont été découvertes dans *InterScan Web Security Virtual Appliance* :
- des comptes avec des privilèges particuliers peuvent télécharger des fichiers système depuis la console ;

- en utilisant des traversées de répertoires et une vulnérabilité permettant l'élévation de privilèges, il est possible d'exécuter des commandes arbitraires ;
- des injections de requêtes illégitimes par rebond sont possibles, ce qui permet notamment de modifier la configuration.

## **5 Solution**

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

## **6 Documentation**

- Bulletin de sécurité Trend Micro du 14 juin 2010 :  
[http://www.trendmicro.com/ftp/documentation/readme/iwsva\\_50\\_ar64\\_en\\_cp1386\\_readme.txt](http://www.trendmicro.com/ftp/documentation/readme/iwsva_50_ar64_en_cp1386_readme.txt)

## **Gestion détaillée du document**

**23 juin 2010** version initiale.