

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans les produits Websense

---

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-2011-AVI-723>

---

### Gestion du document

Référence	CERTA-2011-AVI-723
Titre	Multiples vulnérabilités dans les produits Websense
Date de la première version	26 décembre 2011
Date de la dernière version	–
Source(s)	Note sur le correctif hotfix 24 de Websense
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 ;
- contournement de la politique de sécurité ;
- injection de code indirecte à distance.

## 2 Systèmes affectés

- Websense Webfilter 7.X ;
- Websense Web Security 7.X ;
- Websense Web Security Gateway 7.X.

## 3 Résumé

De multiples vulnérabilités ont été identifiées sur plusieurs produits Websense. Un utilisateur distant malintentionné peut contourner la politique de sécurité, injecter des commandes, et effectuer des injections de code indirecte.

## 4 Description

Plusieurs vulnérabilités ont été identifiées sur les produits Websense. Un utilisateur distant malintentionné peut contourner la politique de sécurité, injecter des commandes, et effectuer des injections de code indirecte. Le site de l'éditeur fournit des informations complémentaires sur ces vulnérabilités.

## 5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation). Websense a publié une mise à jour *Hotfix 24* apportant des corrections à ces problèmes.

## 6 Documentation

- Note sur le correctif hotfix 24 de Websense :  
<http://www.websense.com/support/article/kbarticle/v7-6-About-Hotfix-24-for-Websense-Web-Security-Websense-Web-Filter-and-Web-Security-Gateway>

## Gestion détaillée du document

26 décembre 2011 version initiale.