



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 24 décembre 2007
N° CERTA-2007-AVI-561

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Websense Enterprise

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-2007-AVI-561>

Gestion du document

Référence	CERTA-2007-AVI-561
Titre	Vulnérabilité de Websense Enterprise
Date de la première version	24 décembre 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité Websense KB 976 du 12 décembre 2007
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

Contournement de la politique de sécurité.

2 Systèmes affectés

- Websense Enterprise 6.3.1 ;
- Websense Enterprise 5.5.

3 Résumé

Une vulnérabilité a été identifiée dans l'application Websense Enterprise. Le contenu de requêtes HTTP ne serait pas correctement filtré, ce qui permettrait à un utilisateur de contourner la politique de sécurité mise en place.

4 Description

Une vulnérabilité a été identifiée dans l'application Websense Enterprise. Le contenu de requêtes HTTP ne serait pas correctement filtré. Certains champs `User-Agent` bénéficient d'un traitement privilégié.

Un utilisateur local pourrait donc usurper l'un de ces champs, afin de contourner la politique de filtrage mise en place.

5 Solution

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

6 Documentation

- Bulletin de sécurité Websense KB 976 du 12 décembre 2007 :
<http://www.websense.com/SupportPortal/SupportKbs/976.aspx>
- Annonce de sécurité IBM ISS 39023 du 12 décembre 2007 :
<http://xforce.iss.net/xforce/xfdb/39023>
- Référence CVE CVE-2007-6511 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6511>

Gestion détaillée du document

24 décembre 2007 version initiale.