Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 09 mars 2012
N° CERTA-2012-AVI-128

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Barracuda WAF

Gestion du document

Référence	CERTA-2012-AVI-128
Titre	Vulnérabilité dans Barracuda WAF
Date de la première version	09 mars 2012
Date de la dernière version	–
Source(s)	Avis de sécurité Vulnerability-Lab du 07 mars 2012
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

Injection de code indirecte à distance.

2 Systèmes affectés

Barracuda WAF 660 v7.6.0.028.

3 Résumé

Une vulnérabilité, permettant une injection de code indirecte à distance non persistante, a été corrigée dans *Barracuda WAF*.

4 Description

Cette vulnérabilité peut être utilisée par une personne malveillante à distance pour détourner les sessions. Cependant, cette attaque requiert une interaction avec l'utilisateur. Une exploitation réussie de cette vulnérabilité peut permettre d'obtenir ou de modifier le contexte de l'application de traitement du module pare-feu.

5 Solution

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

6 Documentation

– Avis de sécurité Vulnerability-Lab du 07 mars 2012 :
http://www.vulnerability-lab.com/get_content.php?id=444

Gestion détaillée du document

09 mars 2012 version initiale.