

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans les produits Barracuda Networks

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-2013-AVI-064>

Gestion du document

Référence	CERTA-2013-AVI-064
Titre	Multiples vulnérabilités dans les produits Barracuda Networks
Date de la première version	25 janvier 2013
Date de la dernière version	–
Source(s)	Bulletin de sécurité Barracuda Networks du 23 janvier 2013
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

- Barracuda Spam versions antérieures à 2.0.5
- Barracuda Virus Firewall versions antérieures à 2.0.5
- Barracuda Web Filter versions antérieures à 2.0.5
- Barracuda Message Archiver versions antérieures à 2.0.5
- Barracuda Web Application Firewall versions antérieures à 2.0.5
- Barracuda Link Balancer versions antérieures à 2.0.5
- Barracuda Load Balancer versions antérieures à 2.0.5
- Barracuda SSL VPN versions antérieures à 2.0.5

3 Résumé

De multiples vulnérabilités ont été corrigées dans les produits *Barracuda Networks*. Elles permettent à un attaquant de provoquer un contournement de la politique de sécurité.

4 Solution

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

5 Documentation

- Bulletin de sécurité Barracuda Networks du 23 janvier 2013 :
<https://www.barracudanetworks.com/support/techalerts>

Gestion détaillée du document

25 janvier 2013 version initiale.