



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 08 février 2006
N° CERTA-2006-AVI-062

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités sur Bluecoat ProxySG

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-2006-AVI-062>

Gestion du document

Référence	CERTA-2006-AVI-062
Titre	Vulnérabilités sur Bluecoat ProxySG
Date de la première version	08 février 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité Bluecoat
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

Blue Coat Security Gateway OS (SGOS) versions 4.x antérieures à la version 4.1.4.

3 Résumé

Deux vulnérabilités présentes dans Blue Coat ProxySG peuvent être exploitées par un utilisateur mal intentionné pour contourner la politique de sécurité.

4 Description

- La première vulnérabilité est due à un mauvais traitement sur la méthode `CONNECT`. Cette vulnérabilité permet à un utilisateur mal intentionné d'utiliser cette méthode vers un port arbitraire pour contourner les règles de sécurité mises en place ;

- la seconde vulnérabilité est due à une erreur dans le traitement des règles définies dans le gestionnaire des règles VPM (Visual Policy Manager). Cette vulnérabilité peut également être utilisée pour contourner la politique de sécurité.

5 Solution

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

6 Documentation

- Bulletin de sécurité Blue Coat :
http://www.bluecoat.com/support/knowledge/advisory_connect_denial_ignore.html

Gestion détaillée du document

08 février 2006 version initiale.