Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 02 novembre 2007
N° CERTA-2007-AVI-471

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Blue Coat Security Gateway OS

Gestion du document

Référence	CERTA-2007-AVI-471
Titre	Vulnérabilité de Blue Coat Security Gateway OS
Date de la première version	02 novembre 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité de l'éditeur du 29 octobre 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

- Blue Coat Security Gateway OS versions antérieures à la version 4.2.6.1 ;
- Blue Coat Security Gateway OS versions antérieures à la version 5.2.2.5.

3 Résumé

Une vulnérabilité de type injection de code indirecte (*Cross Site Scripting*) a été découverte dans `Blue Coat Security Gateway OS` (SGOS).

4 Description

Une vulnérabilité de type injection de code indirecte (*Cross Site Scripting*) a été découverte dans l'interprétation de certaines variables faite par les pages *install_upload_action/crl_format* et *install_upload_from_file.htm* de `Blue Coat ProxySG SGOS`.

Cette vulnérabilité peut être exploitée par un utilisateur mal intentionné afin d'exécuter du code HTML ou du script dans le contexte d'un utilisateur visitant un site vulnérable.

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/securityadvisories/advisory_cross-site_scripting_vulnerability

Gestion détaillée du document

02 novembre 2007 version initiale.