

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Bluecoat Reporter

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-2012-AVI-737>

Gestion du document

Référence	CERTA-2012-AVI-737
Titre	Multiples vulnérabilités dans Bluecoat Reporter
Date de la première version	14 décembre 2012
Date de la dernière version	–
Source(s)	Bulletin de sécurité Bluecoat SA71 du 12 décembre 2012 Bulletin de sécurité Bluecoat SA72 du 12 décembre 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

- Atteinte à la confidentialité des données ;
- injection de code indirecte à distance ;
- injection de requêtes illégitime par rebond.

2 Systèmes affectés

Versions antérieures à Bluecoat Reporter 9.3.3.2

3 Résumé

De multiples vulnérabilités ont été corrigées dans *Bluecoat Reporter*. La première concerne la communication de clair des données entre le client et le serveur, un attaquant peut ainsi obtenir le mot de passe de l'administrateur (une attaque par homme du milieu est nécessaire). Les autres vulnérabilités concernent des injections de codes indirectes à distance (XSS) et des injections de requêtes illégitimes par rebond (CSRF).

4 Solution

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

5 Documentation

- Bulletin de sécurité SA71 du 12 décembre 2012 :
<https://kb.bluecoat.com/index?page=content&id=SA71>
- Bulletin de sécurité SA72 du 12 décembre 2012 :
<https://kb.bluecoat.com/index?page=content&id=SA72>

Gestion détaillée du document

14 décembre 2012 version initiale.