

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans des produits BlueCoat

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-2011-AVI-272>

Gestion du document

Référence	CERTA-2011-AVI-272
Titre	Vulnérabilité dans des produits BlueCoat
Date de la première version	04 mai 2011
Date de la dernière version	–
Source	Bulletin de sécurité BlueCoat SA55 du 02 mai 2011
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

Exécution de code arbitraire à distance.

2 Systèmes affectés

Bluecoat BCAA utilisé par les produits :

- ProxySG 6.x, 5.x et 4.x ;
- ProxyOne.

3 Résumé

Une vulnérabilité dans le module BCAA des BlueCoat permet à un utilisateur malveillant d'exécuter du code arbitraire à distance.

4 Description

L'utilisation des relais BlueCoat ProxyOne et ProxySG demande l'installation d'un module BCAA sur un serveur Windows. Ce module utilise un port particulier pour des opérations de synchronisation. L'envoi de paquets

spécialement conçus sur ce port permet à un utilisateur malveillant d'exécuter du code arbitraire à distance sur le serveur Windows.

5 Solution

Les versions 6.2.1.1 et 5.5.5.1 de ProxySG corrigent le problème. Le correctif pour ProxyOne n'est pas encore disponible.

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

6 Documentation

- Bulletin de sécurité BlueCoat SA55 du 02 mai 2011 :
<https://kb.bluecoat.com/index?page=content&id=SA55>

Gestion détaillée du document

04 mai 2011 version initiale.