

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans Blue Coat Director

---

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-524>

---

### Gestion du document

Référence	CERTA-2011-AVI-524
Titre	Multiples vulnérabilités dans Blue Coat Director
Date de la première version	19 septembre 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité Blue Coat SA61 du 13 septembre 2011 Bulletin de sécurité Blue Coat SA62 du 15 septembre 2011 Bulletin de sécurité Blue Coat SA63 du 15 septembre 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 ;
- déni de service à distance ;
- contournement de la politique de sécurité ;
- atteinte à la confidentialité des données ;
- injection de code indirecte à distance.

## 2 Systèmes affectés

Blue Coat Director toutes versions antérieures à la 5.5.2.3.

## 3 Résumé

De multiples vulnérabilités touchent Blue Coat Director, elles permettent notamment l'exécution de code arbitraire à distance.

## 4 Description

Des vulnérabilités dans le module d'analyse des requêtes HTTP TRACE et dans les versions d'Apache et OpenSSL embarquées dans Blue Coat Director permettent à une personne malintentionnée d'effectuer des actions malveillantes, dont l'exécution de code arbitraire à distance.

## 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 SA61 du 13 septembre 2011 :  
<https://kb.bluecoat.com/index?page=content&id=SA61>
- Bulletin de sécurité Blue Coat SA62 du 15 septembre 2011 :  
<https://kb.bluecoat.com/index?page=content&id=SA62>
- Bulletin de sécurité Blue Coat SA63 du 15 septembre 2011 :  
<https://kb.bluecoat.com/index?page=content&id=SA63>
- Référence CVE CVE-2003-0190 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-0190>
- Référence CVE CVE-2005-2666 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-2666>
- Référence CVE CVE-2008-2364 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2364>
- Référence CVE CVE-2008-2939 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2939>
- Référence CVE CVE-2009-1891 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1891>
- Référence CVE CVE-2009-2412 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2412>
- Référence CVE CVE-2009-3094 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3094>
- Référence CVE CVE-2009-3095 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3095>
- Référence CVE CVE-2009-3555 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3555>
- Référence CVE CVE-2009-3560 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3560>
- Référence CVE CVE-2009-3720 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3720>
- Référence CVE CVE-2010-0425 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0425>
- Référence CVE CVE-2010-0434 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0434>
- Référence CVE CVE-2010-1452 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1452>
- Référence CVE CVE-2010-1623 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1623>

## Gestion détaillée du document

19 septembre 2011 version initiale.