



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 janvier 2012
N° CERTA-2012-AVI-015

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Bluecoat PolicyCenter

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-015>

Gestion du document

Référence	CERTA-2012-AVI-015
Titre	Multiples vulnérabilités dans Bluecoat PolicyCenter
Date de la première version	13 janvier 2012
Date de la dernière version	–
Source(s)	Bulletin de sécurité Bluecoat SA64 du 10 janvier 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

- Dénis de service à distance ;
- contournement de la politique de sécurité ;
- élévation de privilèges.

2 Systèmes affectés

Toutes les versions de *Bluecoat PolicyCenter* antérieures à 8.7.2 sont vulnérables. Les versions 8.7.2 et ultérieures le sont également si *Sun Directory Server* est utilisé en version 5.2.

3 Résumé

De multiples vulnérabilités dans *Bluecoat PolicyCenter* permettent de réaliser un déni de service à distance ainsi que des élévations de privilèges.

4 Description

Bluecoat PolicyCenter installe une version vulnérable (5.2) de *Sun Directory Server*. Les failles concernant cette version de logiciel permettent de réaliser un déni de service à distance, ou d'obtenir des droits en lecture et en écriture sur certains fichiers, notamment ceux de configuration.

5 Solution

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

6 Documentation

- Bulletin de sécurité Bluecoat SA64 du 10 janvier 2012 :
<https://kb.bluecoat.com/index?page=content&id=SA64>
- Référence CVE CVE-2006-2513 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2513>
- Référence CVE CVE-2006-3127 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-3127>
- Référence CVE CVE-2006-4175 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4175>
- Référence CVE CVE-2007-2466 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2466>
- Référence CVE CVE-2007-3224 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3224>
- Référence CVE CVE-2007-3225 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3225>
- Référence CVE CVE-2009-0576 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0576>
- Référence CVE CVE-2009-1332 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1332>

Gestion détaillée du document

13 janvier 2012 version initiale.