

Affaire suivie par :  
CERT-FR

## AVIS DU CERT-FR

**Objet : Multiples vulnérabilités dans les produits BlueCoat**

### Gestion du document

Référence	CERTFR-2016-AVI-402
Titre	Multiples vulnérabilités dans les produits BlueCoat
Date de la première version	09 décembre 2016
Date de la dernière version	–
Source(s)	Bulletin de sécurité BlueCoat SA134 du 08 décembre 2016
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(s)

- déni de service à distance
- élévation de privilèges

### 2 - Systèmes affectés

De multiples produits sont impactés. Se référer au bulletin de l'éditeur pour la liste exhaustive des produits.

### 3 - Résumé

De multiples vulnérabilités ont été corrigées dans *les produits BlueCoat*. Elles permettent à un attaquant de provoquer un déni de service à distance et une élévation de privilèges.

### 4 - Solution

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

### 5 - Documentation

- Bulletin de sécurité BlueCoat SA134 du 08 décembre 2016  
<https://bto.bluecoat.com/security-advisory/sa134>

- Référence CVE CVE-2016-5195  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5195>
- Référence CVE CVE-2016-7039  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7039>
- Référence CVE CVE-2016-8666  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-8666>
- Référence CVE CVE-2016-9555  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9555>

## **Gestion détaillée du document**

**09 décembre 2016** version initiale.

---

Conditions d'utilisation de ce document : <http://cert.ssi.gouv.fr/cert-fr/apropos.html>  
Dernière version de ce document : <http://cert.ssi.gouv.fr/site/CERTFR-2016-AVI-402>

---