

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité de Cisco Building Broadband Service Manager

---

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-2008-AVI-256>

---

### Gestion du document

Référence	CERTA-2008-AVI-256
Titre	Vulnérabilité de Cisco Building Broadband Service Manager
Date de la première version	20 mai 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité CISCO via Bugtraq du 14 mai 2008
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

Contournement de la politique de sécurité.

## 2 Systèmes affectés

Cisco Building Broadband Service Manager 5.x.

## 3 Résumé

Une vulnérabilité a été découverte dans Cisco Broadband Service Manager. Elle peut être exploitée afin de réaliser des attaques par injection de code indirecte (*Cross Site Scripting*).

## 4 Description

Une vulnérabilité a été découverte dans la gestion du paramètre *msg* par la page *AccessCodeStart.asp* dans Cisco Broadband Service Manager. Cette vulnérabilité peut être exploitée afin de réaliser une attaque par injection de code indirecte (*Cross Site Scripting*).

## 5 Solution

Appliquer la mise à jour BBSMPatch5332.zip (cf. section Documentation).

## 6 Documentation

- Bulletin de sécurité Cisco (Bugtraq):  
<http://archives.neohapsis.com/archives/bugtraq/2008-05/0183.html>  
<http://archives.neohapsis.com/archives/bugtraq/2008-05/0166.html>
- Mise à jour Cisco :  
[http://tools.cisco.com/support/downloads/go/\[...\]treeName=Network%20Monitoring%20and%20Management](http://tools.cisco.com/support/downloads/go/[...]treeName=Network%20Monitoring%20and%20Management)
- Référence CVE CVE-2008-2165 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-2165>

## Gestion détaillée du document

**20 mai 2008** version initiale.