

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans Cisco Unified MeetingPlace Web Conferencing

---

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-2009-AVI-084>

---

### Gestion du document

Référence	CERTA-2009-AVI-084
Titre	Vulnérabilités dans Cisco Unified MeetingPlace Web Conferencing
Date de la première version	03 mars 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité cisco-sa-20090225-mtgplace du 25 février 2009 Bulletin de sécurité cisco-sr-20090226-mtgplace du 26 février 2009
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

- Accès à distance avec les droits administrateur ;
- contournement de la politique de sécurité ;
- injection de code indirecte.

## 2 Systèmes affectés

*Cisco Unified MeetingPlace Web Conferencing* versions 6.0 et 7.0.

## 3 Résumé

Deux vulnérabilités dans *Cisco Unified MeetingPlace Web Conferencing* permettent d'accéder à distance à l'application avec des droits administrateur et de réaliser des attaques de type *cross-site scripting*.

## 4 Description

Deux vulnérabilités ont été découvertes dans *Cisco Unified MeetingPlace Web Conferencing* :

- un utilisateur malintentionné peut, par le biais d'une requête spécifiquement constituée, contourner le mécanisme d'authentification du serveur et ainsi obtenir un accès à l'application avec des droits d'administration ;
- un utilisateur authentifié peut, par le biais de la page d'édition du compte, réaliser des attaques de type *cross-site scripting*.

## 5 Solution

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

## 6 Documentation

- Bulletin de sécurité Cisco 20090225-mtgplace du 25 février 2009 :  
<http://www.cisco.com/warp/public/707/cisco-sa-20090225-mtgplace.shtml>
- Bulletin de sécurité Cisco 20090226-mtgplace du 26 février 2009 :  
<http://www.cisco.com/warp/public/707/cisco-sr-20090226-mtgplace.shtml>
- Référence CVE-2009-0614 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0614>

## Gestion détaillée du document

**03 mars 2009** version initiale.