Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 29 janvier 2010
N° CERTA-2010-AVI-034

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Cisco Unified MeetingPlace

Gestion du document

Référence	CERTA-2010-AVI-034
Titre	Multiples vulnérabilités dans Cisco Unified MeetingPlace
Date de la première version	29 janvier 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco cisco-sa-20100127-mp du 27 janvier 2010
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 ;
- atteinte à l'intégrité des données ;
- atteinte à la confidentialité des données ;
- élévation de privilèges.

2 Systèmes affectés

- Cisco Unified MeetingPlace versions 5.x ;
- Cisco Unified MeetingPlace versions 6.x ;
- Cisco Unified MeetingPlace versions 7.x.

3 Résumé

De multiples vulnérabilités ont été découvertes dans `Cisco Unified MeetingPlace`. L'exploitation de ces vulnérabilités permet de réaliser différentes actions malveillantes, allant jusqu'à l'élévation de privilèges.

4 Description

Quatre vulnérabilités ont été découvertes dans `Cisco Unified MeetingPlace`:

- la première est due à une erreur dans la gestion des requêtes `SQL` et peut être exploitée afin d'injecter du code `SQL` arbitraire ;
- la deuxième est due à une erreur dans la gestion des requêtes à destination de l'interface interne du serveur web. L'exploitation de cette vulnérabilité permet de contourner les mécanismes de sécurité ;
- la troisième et la quatrième vulnérabilité sont dues à des erreurs dans le mécanisme d'authentification `MeetingTime` et peuvent être exploitées afin de récupérer des couples d'authentification et/ou d'élever ses privilèges au niveau administrateur.

5 Solution

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

6 Documentation

- Bulletin de sécurité Cisco 20100127-mp du 27 janvier 2010 :
  http://www.cisco.com/warp/public/707/cisco-sa-20100127-mp.shtml
- Référence CVE CVE-2010-0139 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0139
- Référence CVE CVE-2010-0140 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0140
- Référence CVE CVE-2010-0141 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0141
- Référence CVE CVE-2010-0142 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0142

Gestion détaillée du document

29 janvier 2010 version initiale.