

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Cisco WebEx WRF Player

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-550>

Gestion du document

Référence	CERTA-2009-AVI-550
Titre	Multiples vulnérabilités dans Cisco WebEx WRF Player
Date de la première version	17 décembre 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité cisco-sa-20091216-webex du 16 décembre 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

Exécution de code arbitraire à distance.

2 Systèmes affectés

- Cisco WebEx WRF Player pour Windows versions antérieures à 26.49.32 (branche 26.x) et à 27.10.x (branche 27.x);
- Cisco WebEx WRF Player pour Mac OS X versions antérieures à 26.49.35 (branche 26.x) et à 27.11.8 (branche 27.x);
- Cisco WebEx WRF Player pour Linux versions antérieures à 26.49.35 (branche 26.x) et à 27.11.8 (branche 27.x).

3 Résumé

De multiples vulnérabilités dans Cisco WebEx WRF Player permettent d'exécuter du code arbitraire à distance.

4 Description

WebEx Recording Format (WRF) est un format de fichier utilisé pour les enregistrements de réunion WebEx. *Cisco WebEx WRF Player* est une application utilisée pour lire et éditer des fichiers au format WRF. Le lecteur *WRF Player* peut être téléchargé automatiquement lorsqu'un utilisateur accède à un fichier au format WRF hébergé sur un serveur WebEx. Ce lecteur peut également être installé manuellement.

De multiples vulnérabilités permettant l'exécution de code arbitraire à distance ont été découvertes dans *Cisco WebEx WRF Player*.

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 20091216-webex du 16 décembre 2009 :
<http://www.cisco.com/warp/public/707/cisco-sa-20091216-webex.shtml>
- Référence CVE CVE-2009-2875 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2875>
- Référence CVE CVE-2009-2876 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2876>
- Référence CVE CVE-2009-2877 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2877>
- Référence CVE CVE-2009-2878 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2878>
- Référence CVE CVE-2009-2879 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2879>
- Référence CVE CVE-2009-2880 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2880>

Gestion détaillée du document

17 décembre 2009 version initiale.