



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 19 août 2003
N° CERTA-2003-AVI-137

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités de l'application CiscoWorks

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-2003-AVI-137>

Gestion du document

Référence	CERTA-2003-AVI-137
Titre	Vulnérabilités de l'application CiscoWorks
Date de la première version	19 août 2003
Date de la dernière version	–
Source(s)	Avis de sécurité Cisco #44502
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

- Elévation de privilèges ;
- exécution de code arbitraire.

2 Systèmes affectés

CiscoWorks Common Management Foundation (CMF) versions 2.1 et antérieures.

L'application CiscoWorks CMF est intégrée dans les produits suivants :

- toutes les versions de CiscoWorks CD 1 ;
- Ressource Manager Essentials (RME) versions 2.0, 2.1 et 2.2 ;
- Cisco Ressource Manager (CRM) versions 1.0 et 1.1.

3 Résumé

Deux vulnérabilités de CiscoWorks CMF permettent à un utilisateur local mal intentionné d'obtenir les privilèges de l'administrateur ou d'exécuter du code arbitraire sur le serveur hébergeant l'application CiscoWorks.

4 Description

La première vulnérabilité permet à un utilisateur non privilégié de l'application CiscoWorks - y compris le compte *invité* s'il est activé - d'obtenir les droits de l'administrateur par le biais d'une URL malicieusement constituée.

La deuxième vulnérabilité permet à un utilisateur de l'application CiscoWorks d'exécuter du code arbitraire sur le serveur hébergeant cette application, avec les privilèges de l'utilisateur "*casuser*", sous lequel tourne l'application CiscoWorks.

5 Contournement provisoire

Pour limiter le risque d'exploitation de la première vulnérabilité, il est recommandé de désactiver le compte *invité*.

6 Solution

La version CiscoWorks CMF 2.2 corrige ces deux vulnérabilités.

7 Documentation

Avis de sécurité Cisco #44502 :

<http://www.cisco.com/warp/public/707/cisco-sa-20030813-cmf.shtml>

Gestion détaillée du document

19 août 2003 version initiale.