



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 juillet 2006
N° CERTA-2006-AVI-292

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité sur Cisco Router Web Setup (CWRS)

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-2006-AVI-292>

Gestion du document

Référence	CERTA-2006-AVI-292
Titre	Vulnérabilité sur Cisco Router Web Setup (CWRS)
Date de la première version	13 juillet 2006
Date de la dernière version	-
Source(s)	Bulletin de sécurité CISCO
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 ;
- déni de service ;
- élévation de privilèges.

2 Systèmes affectés

Tous les routeurs Cisco avec une version IOS antérieure à la version 3.3.0 build 31.

3 Résumé

Une vulnérabilité sur l'application Cisco Router Web Setup (CWRS) peut être exploitée par un utilisateur mal intentionné pour exécuter du code arbitraire sur un routeur ayant la configuration par défaut du routeur et la version vulnérable de l'IOS.

4 Description

L'application CWRS est une application graphique destinée à configurer les routeurs Cisco series 800 et Cisco SOHO. Cette application est appelée à partir du serveur web CISCO IOS HTTP.

Une vulnérabilité sur l'authentification par défaut (login / mot de passe) sur le logiciel CWRS peut être exploitée par un utilisateur mal intentionné pour exécuter des commandes arbitraires avec les privilèges de niveau 15 (les privilèges de niveau 15 étant les plus hauts privilèges sur un produit géré par Cisco IOS).

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 ID 20060712-crws du 12 juillet 2006 :
<http://www.cisco.com/warp/public/707/cisco-sa-20060712-crws.shtml>

Gestion détaillée du document

13 juillet 2006 version initiale.