Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 20 avril 2006
N° CERTA-2006-AVI-168

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Cisco CiscoWorks WLSE

Gestion du document

Référence	CERTA-2006-AVI-168
Titre	Vulnérabilités dans Cisco CiscoWorks WLSE
Date de la première version	20 avril 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité de l'éditeur 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

Élévation de privilèges.

2 Systèmes affectés

Les versions CiscoWorks Wireless LAN Solution Engine (WLSE) et CiscoWorks WLSE Express antérieures à 2.13.

3 Résumé

Des vulnérabilités existent dans certaines versions de Cisco Wireless LAN Solution Engine (WLSE) et WLSE Express. Un utilisateur malveillant peut utiliser l'une de ces vulnérabilités pour élever ses privilèges à ceux d'administrateur.

4 Description

Cisco Wireless LAN Solution Engine (WLSE) est une application permettant de gérer et surveiller une infrastructure sans-fil Cisco. Deux vulnérabilités existent dans les versions de cette application antérieures à 2.13 :

– l'interface web des utilisateurs peut être utilisée par un utilisateur malveillant pour faire une injection de code

indirecte (`Cross Site Scripting`), lui permettant d'obtenir des informations de sessions suffisantes pour acquérir les droits de l'administrateur du système.
– l'interface de commandes en ligne peut fournir un compte administrateur à un utilisateur ayant accès à cette interface et renseignant une commande particulière.

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 69920 du 19 avril 2006 :
http://www.cisco.com/warp/public/707/cisco-sa-20060419-wlse.shtml
– Bulletin de sécurité Cisco ID 69930 du 19 avril 2006 :
http://www.cisco.com/warp/public/707/cisco-sr-20060419-priv.shtml

Gestion détaillée du document

20 avril 2006 version initiale.