Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 08 avril 2004
N° CERTA-2004-AVI-118

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans les équipements WLSE et HSE de Cisco

Gestion du document

Référence	CERTA-2004-AVI-118
Titre	Vulnérabilité dans les équipements WLSE et HSE de Cisco
Date de la première version	08 avril 2004
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco SA-20040407
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

Prise de contrôle de l'équipement à distance.

2 Systèmes affectés

- Equipement WLSE avec les versions de logiciel 2.0, 2.0.2 et 2.5 ;
- équipement HSE avec les versions de logiciel 1.7, 1.7.1, 1.7.2 et 1.7.3.

3 Résumé

La présence d'un compte possédant un mot de passe par défaut sur les équipements WLSE et HSE permet leur prise de contrôle à distance.

4 Description

L'équipement CiscoWorks WLSE (Wireless LAN Solution Engine) permet l'administration centralisée des infrastructures Cisco Wireless LAN.

L'équipement HSE (Hosting Solution Engine) permet de contrôler des services de type `e-business`.

Ces deux équipements contiennent un compte utilisateur par défaut ne pouvant pas être désactivé. Un mot de passe par défaut est associé à ce compte. L'utilisation de ce compte permet la prise de contrôle à distance de ces équipements.

5 Solution

Se référer au bulletin de sécurité du constructeur (cf. section Documentation) pour l'obtention d'un correctif.

6 Documentation

Bulletin de sécurité Cisco SA-20040407 :
http://www.cisco.com/warp/public/707/cisco-sa-20040407-username.shtml

Gestion détaillée du document

08 avril 2004 version initiale.