Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 28 juin 2001
N° CERTA-2001-AVI-071

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du serveur HTTP IOS

Gestion du document

Référence	CERTA-2001-AVI-071
Titre	Vulnérabilité du serveur HTTP IOS
Date de la première version	28 juin 2001
Date de la dernière version	–
Source(s)	Avis Cisco: "IOS HTTP Authorization Vulnerability"
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

L'exploitation de cette vulnérabilité permet à un utilisateur mal intentionné d'exécuter des commandes avec le plus haut niveau de privilège .

2 Systèmes affectés

Tout équipement CISCO utilisant une version d'IOS 11.3 et suivantes.

3 Résumé

Une vulnérabilité dans le serveur HTTP d'IOS permet à un utilisateur mal inténtionné d'exécuter des commandes avec le plus haut niveau de privilège et ainsi visualiser ou modifier la configuration du périphérique Cisco.

4 Description

Deux conditions doivent être réunies afin d'exploiter la vulnérabilité:

– le serveur HTTP doit être démarré,

– le mode d'authentification doit être de type local, c'est-à-dire que les noms d'utilisateurs et les mots de passe sont définis sur le périphérique lui même.

En envoyant une URL particulière (un seul champ de cette URL prend une valeur aléatoire, un nombre entre 16 et 99 dépendant de la plateforme considérée), il est possible de contourner l'authentification et d'exécuter n'importe quelle commande sur l'équipement.

Les commandes sont exécutées avec le plus haut niveau de privilège (level 15), permettant à l'utilisateur de visualiser et de modifier la configuration de l'équipement.

5 Contournement provisoire

CISCO préconise deux mesures:

– ne pas démarrer HTTP: rajouter la directive `no ip http server` dans le fichier de configuration
– utiliser TACACS+ ou RADIUS pour l'authentification.

6 Solution

Télécharger une mise-à-jour du logiciel IOS sur le site de Cisco:
http://www.cisco.com

7 Documentation

Avis Cisco "IOS HTTP Authorization Vulnerability":
http://www.cisco.com/warp/public/707/IOS-httplevel-pub.html

Gestion détaillée du document

28 juin 2001 version initiale.