Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 21 septembre 2001
N° CERTA-2001-AVI-097

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités de SSH sur CISCO

Gestion du document

Référence	CERTA-2001-AVI-097
Titre	Vulnérabilités de SSH sur CISCO
Date de la première version	21 septembre 2001
Date de la dernière version	–
Source(s)	Bulletin de securite 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

- Modification de la configuration.
- Perte de confidentialité.
- Usurpation d'identité.

2 Systèmes affectés

Parmi les produits CISCO :

- Toutes les versions de CISCO IOS 12.0 et suivantes supportant SSH sont vulnérables.
- Les versions Pix Firewall 5.2 et 5.3 sont affectées.
- Il en est de même pour Cat OS 6.2 sur Catalyst 6000.
- Enfin Sur CSS11000 toutes les versions de WebNS strictement antérieures à R4.01 B42s, R4.10 B22s, R5.0 B11s et 5.01 B6s sont touchées par cette vulnérabilité.

3 Description

Des vulnérabilités du protocole SSH 1.5 permettent à un utilisateur mal intentionné d'introduire des commandes SSH dans une session en cours et d'obtenir des informations permettant de faciliter l'attaque des clés par force brute.

Certains produits des gammes IOS, PIX, Cat OS et CSS11000 sont équipés de ce protocole et sont par conséquent vulnérables.

4 Solution

Appliquer les correctifs de CISCO selon les produits et leurs versions sur le site de CISCO :
http://www.cisco.com

- Pour Cat OS passer à la version 6.1(2.13), 6.2(0.111) et 6.3(0.7)PAN
- WebNS passer aux versions R4.01 B42s, R4.10 B22s, R5.0 B11s et 5.01 B6s.
- pour PIX passer aux versions 5.2(6), 5.3(2) ou 6.0(1).
- Pour IOS passer aux versions indiquées dans le tableau récapitulatif du bulletin CISCO dont l'adresse est indiquée dans le paragraphe Documentation.

5 Documentation

Le bulletin de sécurité CISCO :
http://www.cisco.com/warp/public/707/SSH-multiple-pub.html

Gestion détaillée du document

21 septembre 2001 version initiale.