Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 29 novembre 2001
N° CERTA-2001-AVI-154

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de CBAC sous CISCO IOS

Gestion du document

Référence	CERTA-2001-AVI-154
Titre	Vulnérabilité de CBAC sous CISCO IOS
Date de la première version	29 novembre 2001
Date de la dernière version	–
Source(s)	Bulletin de sécurité CISCO : « A vulnerability in IOS Firewall Feature Set »
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

Contournement des règles de filtrage des routeurs.

2 Systèmes affectés

Les systèmes affectés sont les routeurs CISCO possédant *IOS Firewall Feature Set*, aussi appelé *CISCO Secure Integrated Software*, ou encore *Context Based Access Control* (`CBAC`) inclus dans IOS depuis sa version 11.2p.

Pour être affectés, le fichier de configuration du routeur doit contenir les lignes servant à appliquer les règles `ip inspect`.

(Pour déterminer si un routeur supporte CBAC, le nom de son fichier image contient un « o », comme dans `c2600-io3-m` par exemple).

3 Résumé

Il est possible d'envoyer depuis l'extérieur d'un réseau filtré par CBAC des données non autorisées.

4 Description

CBAC est un complément d'IOS permettant d'établir des ACL (*Access Control Lists* ou règles de filtrage) dynamiques sur un routeur.

Lorsque une connexion est établie vers l'extérieur d'un réseau filtré par le routeur, une ACL dynamique est mise en place, et autorise le trafic entrant correspondant à cette session.

Une vulnérabilité dans la gestion de ces ACL dynamiques permet de contourner le filtrage. Lors du filtrage du trafic, seuls les adresses sources et destination et le numéros de ports sont vérifiés, et pas le protocole utilisé. Il est donc possible d'envoyer un paquet de type différent dans le réseau filtré par le routeur.

5 Solution

Appliquer les correctifs comme indiqué dans le bulletin de sécurité CISCO (voir la section Documentation).

6 Documentation

Bulletin de sécurité de CISCO :
http://www.cisco.com/warp/public/707/IOS-cbac-dynacl/pub.shtml

Gestion détaillée du document

29 novembre 2001 version initiale.