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 novembre 2001
N° CERTA-2001-AVI-144

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités liées aux ACL dans les routeurs CISCO 12000

Gestion du document

Référence	CERTA-2001-AVI-144
Titre	Vulnérabilités liées aux ACL dans les routeurs CISCO 12000
Date de la première version	20 novembre 2001
Date de la dernière version	–
Source(s)	Bulletin de sécurité 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

Contournement des règles de filtrage des routeurs.

2 Systèmes affectés

Routeurs CISCO de la série 12000 uniquement.

3 Résumé

Sur les CISCO de la série 12000, dans certaines conditions, les ACL (Liste de Contrôles d'Accès) mises en place ne sont pas correctement prises en compte.

4 Description

Plusieurs vulnérabilités concernant les ACL sur les routeurs CISCO de la série 12000 sont à corriger.

– Les ACL ne permettent de bloquer que le premier élément d'un paquet fragmenté. Il est donc possible de contourner les règles de sécurité du routeur en dissimulant du trafic malveillant dans certains des fragments.

- Le mot clé `fragment` dans les ACL est ignoré si le paquet est destiné au routeur lui même. Le routeur n'est donc pas protégé par ses ACL.
- Ce mot clé est ignoré dans les ACL s'appliquant aux paquets sortants, une règle contenant ce mot clé ne s'applique que sur les paquets entrants.
  Il peut même arriver que ce mot clé soit ignoré dans tous les cas.
- Une règle implicite `deny ip any any` placée en fin d'une ACL d'exactement 448 entrées appliquée à une interface (contrôle d'accès du trafic sortant) sera ignorée.
- Une ACL risque de ne pas bloquer certains paquets du trafic sortant, si une autre liste concernant le trafic entrant existe mais n'est pas appliquée à toutes les interfaces d'un système de type *Engine 2* uniquement.

5 Solution

Appliquer les correctifs comme indiqué dans l'avis de CISCO. (cf. Section Documentation)

6 Documentation

Avis de sécurité de CISCO :
http://www.cico.com/warp/public/707/GSR-ACL-pub.shtml

Gestion détaillée du document

20 novembre 2001 version initiale.