Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 25 novembre 2005
N° CERTA-2005-AVI-470

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du pare-feu PIX de CISCO

Gestion du document

Référence	CERTA-2005-AVI-470
Titre	Vulnérabilité du pare-feu PIX de CISCO
Date de la première version	25 novembre 2005
Date de la dernière version	–
Source(s)	Forum de discussion Full-disclosure
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

Déni de service.

2 Systèmes affectés

Cisco Pix version 6.3 et 7.0.

3 Résumé

Une vulnérabilité présente sur le pare-feu PIX de CISCO permet à un utilisateur mal intentionné de réaliser un déni de service via des paquets malcieusement construits.

4 Description

Un utilisateur mal intentionné peut réaliser un déni de service via l'utilisation d'un paquet TCP-SYN malicieusement construit ayant une somme de contrôle invalide.

Ce déni de service, d'une durée limitée liée à la configuration du PIX, est restreint aux paquets ayant les mêmes adresses IP, ports sources et destinations que le paquet malicieusement construit.

5 Contournement provisoire

Il n'existe pour le moment aucun correctif à cette vulnérabilité, cependant CISCO a proposé plusieurs solutions permettant de contourner le problème :

- activer le mode « TCP-intercept » ;
- réduire le temps de mise à l'écart associé aux nouvelles connexions bloquées.

6 Documentation

- Information sur le Forum de discussion « Full-Disclosure »
  http://lists.grok.org.uk/pipermail/full-disclosure/2005-November/038983.html
- CISCO Bugid CSCsc14915 :
  http://www.cisco.com/pcgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc14915
- CICSO Bugid CSCsc16014 :
  http://www.cisco.com/pcgi-bin/Support/Bugtool/onebug.pl?bugid=CSCsc16014
- Bulletin de sécurité de US/CERT 853540 :
  http://www.kb.cert.org/vuls/id/853540

Gestion détaillée du document

25 novembre 2005 version initiale.