Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 03 janvier 2005
N° CERTA-2004-AVI-143-004

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans le protocole TCP

Gestion du document

Référence	CERTA-2004-AVI-143-004
Titre	Vulnérabilité dans le protocole TCP
Date de la première version	26 avril 2004
Date de la dernière version	03 janvier 2005
Source(s)	Avis #236929 du NISCC
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

- Toutes les versions de CISCO IOS ;
- CISCO IOS Firewall ;
- tous les pare-feux CheckPoint Firewall-1 antérieurs à la version R55 HFA-03 ;
- tous les routeurs Juniper série M, T et E ;
- tous les pare-feux NetScreen possèdant une version de ScreenOS antérieure à 5.0R6 ;
- NetBSD 1.5.x et 2.0 ;
- SGI IRIX.

3 Résumé

Une faiblesse dans la mise en œuvre du protocole TCP (Transport Control Protocol) a été découverte.

4 Description

TCP (Transport Control Protocol) est un protocole réseau assurant le service de transport en mode connecté. Il est définit par la RFC 793 de l'IETF (Internet Engineering Task Force) et les extensions concernant la haute disponibilité par la RFC 1323.

Une vulnérabilité dans sa mise en œuvre permet à un individu mal intentionné d'effectuer un déni de service sur les connexions TCP préalablement établies par l'envoi de paquets TCP judicieusement formés.

5 Solution

Appliquer le correctif suivant le système utilisé :

- Avis de sécurité Checkpoint :
  http://www.checkpoint.com/techsupport/alerts/tcp_dos.html
- Avis de sécurité CISCO :
  http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml
  http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml
- Avis de sécurité #20040403-01-A de SGI :
  ftp://patches.sgi.com/support/free/security/advisories/20040403-01-A.asc
- Alerte de sécurité Juniper :
  http://www.juniper.net/support/alert.html
- Avis de sécurité NetBSD-SA2004-006 de NetBSD :
  ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2004-006.txt.asc

6 Documentation

- RFC 793 Transmission Control Protocol :
  http://www.ietf.org/rfc/rfc793.txt
- RFC 1323 TCP Extensions for High Performance :
  http://www.ietf.org/rfc/rfc1323.txt
- Bulletin #236929 du NISCC :
  http://www.uniras.gov.uk/vuls/2004/236929/index.htm
- Avis de sécurité FreeBSD du 23 avril mai 2004 :
  http://www.vuxml.org/freebsd/
- Avis de sécurité Novell (Netware 5.x et Netware 6.x) :
  http://support.novell.com/cgi-bin/search/searchtid.cgi?/10092941.htm
- Bulletin de sécurité HP HPSBTU01077 "HP Tru64 UNIX TCP stack remote denial of service (DoS)" du 22 décembre 2004 :
  http://www5.itrc.hp.com/service/cki/docDisplay.do?docId=HPSBTU01077
- Référence CVE CAN-2004-0230 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0230

Gestion détaillée du document

26 avril 2004 version initiale.

27 avril 2004 retrait de l'avis SUN.

12 mai 2004 ajout de la référence au bulletin de sécurité FreeBSD.

24 mai 2004 ajout de l'avis de sécurité Novell.

03 janvier 2005 ajout référence au bulletin de sécurité HP HPSBTU01077 pour Tru64 UNIX .