

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité de l'option TCP Timestamp sur plusieurs produits Cisco

---

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>  
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2005-AVI-173>

---

### Gestion du document

Référence	CERTA-2005-AVI-173-001
Titre	Vulnérabilité de l'option TCP Timestamp sur plusieurs produits Cisco
Date de la première version	23 mai 2005
Date de la dernière version	27 mai 2005
Source(s)	Avis de sécurité Cisco du 18 mai 2005
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

- Routeurs de la série Cisco SN5400 ;
- commutateurs de la série Cisco CSS1000 ;
- points d'accès de la série Cisco Aironet 1200 ;
- points d'accès de la série Cisco Aironet 350 ;
- commutateurs WAN de la série Cisco MGX.

## 3 Description

Certaines implémentations de l'option *Timestamp* du protocole TCP sont vulnérables à un déni de service. Des paquets malicieusement construits envoyés sur un équipement vulnérable peuvent bloquer une connexion TCP prédéterminée.

## 4 Solution

Se référer au bulletin de sécurité du constructeur pour l'obtention du correctif.

## 5 Documentation

- Bulletin de sécurité Cisco "Vulnerability in a Variant of the TCP timestamps option" :  
<http://cisco.com/warp/public/707/cisco-sn-20050518-tcpts.shtml>
- Référence CVE CAN-2005-0356 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0356>

## Gestion détaillée du document

**23 mai 2005** version initiale.

**27 mai 2005** ajout de la référence CVE.