

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Cisco Wide Area Application Services (WAAS)

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-2007-AVI-321>

Gestion du document

Référence	CERTA-2007-AVI-321
Titre	Vulnérabilité dans Cisco Wide Area Application Services (WAAS)
Date de la première version	19 juillet 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité CISCO 92020 publié le 18 juillet 2007
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 à distance.

2 Systèmes affectés

– Les logiciels CISCO WAAS dont les versions sont comprises entre 4.0.7 et 4.0.9 incluse.

Cette vulnérabilité concerne les WAE Appliance et le module de réseau NM-WAE-502, qui sont configurés avec Edge Services et l'optimisation CIFS. Les adresses en référence fournissent les commandes permettant de vérifier si de telles options de configuration sont utilisées.

3 Résumé

Une vulnérabilité a été identifiée dans le service Wide Area Application (WAAS) de Cisco. Une personne malveillante pourrait l'exploiter afin d'empêcher le système vulnérable de gérer le trafic de données et le trafic de gestion.

4 Description

Une vulnérabilité a été identifiée dans le service Wide Area Application (WAAS) de Cisco. Ce logiciel offre des techniques pour optimiser le temps de latence du transport de différents flux ainsi que l'occupation de la bande passante. Il s'installe sur une combinaison de produits Cisco, directement dans le WAE (pour Wide Area Application Engine) et sous forme de module sur d'autres équipements comme des NAS (Network Access Server).

Le WAAS pourrait être perturbé par l'envoi massif de paquets TCP d'établissement de connexion (SYN) vers les ports 139 ou 445. Ces ports sont utilisés pour la fonctionnalité CIFS du logiciel. Une personne malveillante pourrait ainsi exploiter cette vulnérabilité en inondant le WAAS de tels paquets, l'empêchant de gérer le trafic de données et le trafic de gestion.

5 Solution

Se référer au bulletin de sécurité de Cisco pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Cisco ID 92020 du 18 juillet 2007 :
<http://www.cisco.com/warp/public/707/cisco-sa-20070718-waas.shtml>
- Note d'information Cisco ID 97398 du 18 juillet 2007 proposant quelques mesures de contournement :
http://www.cisco.com/en/US/products/products_applied_intelligence_response09186a0080883ccf.html

Gestion détaillée du document

19 juillet 2007 version initiale.