Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 août 2010
N° CERTA-2010-AVI-381

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Cisco ACE

Gestion du document

Référence	CERTA-2010-AVI-381
Titre	Vulnérabilités dans Cisco ACE
Date de la première version	13 août 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco 20100811-ace du 11 août 2010
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

- Cisco ACE Application Control Engine Module ;
- Cisco ACE 4710 Application Control Engine.

3 Résumé

Plusieurs vulnérabilités dans les produits Cisco ACE permettent à un utilisateur malintentionné de réaliser un déni de service à distance.

4 Description

Plusieurs vulnérabilités dans les produits Cisco ACE permettent à un utilisateur malintentionné de réaliser un déni de service à distance :

- (CVE-2010-2822) le traitement de l'inspection des flux RTSP en transit par les modules et les boîtiers ACE présente une erreur. Cette inspection des flux RTSP n'est pas activée par défaut ;

- (CVE-2010-2823) les boîtiers Cisco ACE 4710 présentent un défaut lors de l'inspection en profondeur des flux HTTP en transit. Cette vulnérabilité est présente dès lors que l'inspection des flux HTTP, RTSP ou SIP est activée. L'inspection des flux HTTP, RTSP et SIP n'est pas activée par défaut ;
- (CVE-2010-2824) le module Cisco ACE peut cesser de fonctionner quand certains paquets SSL spécialement conçus lui sont adressés ;
- (CVE-2010-2825) des paquets SIP en transit spécialement conçus peuvent provoquer un arrêt de fonctionnement des modules et des boîtiers Cisco ACE quand l'inspection de ce flux est activée. L'inspection des flux SIP n'est pas activée par défaut.

5 Solution

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

6 Documentation

- Bulletin de sécurité Cisco 20100811-ace du 11 août 2010 :
  http://www.cisco.com/warp/public/707/cisco-sa-20100811-ace.shtml
- Référence CVE CVE-2010-2822 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2822
- Référence CVE CVE-2010-2823 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2823
- Référence CVE CVE-2010-2824 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2824
- Référence CVE CVE-2010-2825 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2825

Gestion détaillée du document

13 août 2010 version initiale.