

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité 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-2007-AVI-191>

Gestion du document

Référence	CERTA-2007-AVI-191
Titre	Vulnérabilité CISCO
Date de la première version	26 avril 2007
Date de la dernière version	–
Source(s)	
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

Exécution de code arbitraire.

2 Systèmes affectés

- CISCO Network Analysis Modules 6000, 6500, 7600 ;
- CISCO Unified Application Environment versions 2.x ;
- CISCO Hosting Solution Engine versions 1.x ;
- CISCO Hosting Solution Software versions 1.x.

3 Résumé

Une vulnérabilité présente dans plusieurs produits CISCO pourrait conduire à l'exécution de code arbitraire sur des produits vulnérables. Cette vulnérabilité provient du module PHP et plus particulièrement des fonctions `htmlentities()` et `htmlspecialchars()` qui ne gèrent pas correctement des données mal formées provoquant ainsi un débordement de tampon.

4 Solution

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

5 Documentation

- Bulletin de sécurité Cisco ID 82377 du 25 avril 2007 :
<http://www.cisco.com/warp/public/707/cisco-sr-20070425-http.shtml>
- Référence CVE CAN-2006-5465 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2006-5465>

Gestion détaillée du document

26 avril 2007 version initiale.