

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité sur les produits CISCO TACAS+

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-2006-AVI-079>

Gestion du document

Référence	CERTA-2006-AVI-079
Titre	Vulnérabilité sur les produits CISCO TACAS+
Date de la première version	16 février 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité CISCO 20060215
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

Contournement de la politique de sécurité.

2 Systèmes affectés

- Cisco Guard 5.x ;
- Cisco Traffic Anomaly Detector 5.x ;
- Cisco Catalyst 6500 Router Anomaly Guard Module ;
- Cisco Catalyst 7600 Router Anomaly Guard Module ;
- Cisco Catalyst 6500 Router Traffic Anomaly Detector Module ;
- Cisco Catalyst 7600 Router Traffic Anomaly Detector Module.

3 Description

Une vulnérabilité présente dans les produits CISCO TACAS+ (Terminal Access Controller Access Control System Plus) peut être utilisée par un utilisateur mal intentionné pour contourner la politique de sécurité du système.

4 Solution

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

5 Documentation

- Site Internet de CISCO :
<http://www.cisco.com/>
- Bulletin de sécurité Cisco ID XXXXX du 15 février 2006 :
<http://www.cisco.com/warp/public/707/cisco-sa-20060215-guard.shtml>

Gestion détaillée du document

16 février 2006 version initiale.