

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans les 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-431>

Gestion du document

Référence	CERTA-2005-AVI-431
Titre	Vulnérabilité dans les produits Cisco
Date de la première version	03 novembre 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco #20051102-timers du 02 novembre 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 ;
- Exécution de code arbitraire à distance.

2 Systèmes affectés

- Cisco IOS 12.0 ;
- Cisco IOS 12.1 ;
- Cisco IOS 12.2 ;
- Cisco IOS 12.3 ;
- Cisco IOS 12.4.

3 Résumé

Une vulnérabilité dans les produits Cisco équipés d'un IOS (Internal Operating System) permet à un utilisateur distant de provoquer un déni de service ou d'exécuter du code arbitraire.

4 Description

Une erreur dans la mise en œuvre des *timers* internes des IOS Cisco permet d'exécuter du code arbitraire précédemment injecté en mémoire par une attaque de type débordement de tas (*heap overflow*). Ceci permet à un utilisateur distant mal intentionné de provoquer un déni de service ou d'exécuter du code arbitraire à distance en exploitant cette vulnérabilité combinée à une autre de type *heap overflow* comme celle décrite dans l'avis CERTA-2005-AVI-309 sur la pile IPv6 des équipements Cisco.

5 Solution

Se référer au bulletin de sécurité Cisco pour appliquer le correctif approprié (cf. Documentation).

6 Documentation

- Site de l'éditeur :
<http://www.cisco.com>
- Bulletin de sécurité Cisco #20051102-timers du 02 novembre 2005 :
<http://www.cisco.com/warp/public/707/cisco-sa-20051102-timers.shtml>
- Avis CERTA-2005-AVI-309 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2005-AVI-309/CERTA-2005-AVI-309.html>

Gestion détaillée du document

03 novembre 2005 version initiale.