Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 17 octobre 2002
N° CERTA-2002-AVI-231

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du serveur HTTP des commutateurs Catalyst de 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-2002-AVI-231`

Gestion du document

Référence	CERTA-2002-AVI-231
Titre	Vulnérabilité du serveur HTTP des commutateurs Catalyst de Cisco
Date de la première version	17 octobre 2002
Date de la dernière version	–
Source(s)	Avis de Sécurité "Cisco CatOS Embedded HTTP Server Buffer Overflow" de Cisco
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.

2 Systèmes affectés

Tous les commutateurs Catalyst utilisant une version de CatOS comprise entre les versions 5.4 et 7.3 incluse avec les caractères `cv` présents dans le nom de l'image.

3 Résumé

Une vulnérabilité présente dans le service HTTP permet à un utilisateur mal intentionné de forcer, à distance, le redémarrage des commutateurs.

4 Description

Certains commutateurs Cisco de la série Catalyst possèdent un serveur HTTP utilisé par le logiciel Cisco View (supervision de réseaux).

Une vulnérabilité de type débordement de mémoire est présente dans ce serveur HTTP et permet à un utilisateur mal intentionné de forcer, à distance, le redémarrage du commutateur (`reset`).

5 Contournement provisoire

- Ne pas démarrer le serveur HTTP si celui-ci n'est pas utilisé ;
- Filtrer le port 80/TCP (HTTP) sur le garde barrière afin d'éviter une attaque provenant de l'extérieur.

6 Solution

Se référer au bulletin de sécurité Cisco (cf. section Documentation) pour l'obtention d'un correctif.

7 Documentation

Avis de Sécurité "Cisco CatOS Embedded HTTP Server Buffer Overflow" de Cisco :
http://www.cisco.com/warp/public/707/catos-http-overflow-vuln.shtml

Gestion détaillée du document

17 octobre 2002 version initiale.