Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 06 avril 2006
N° CERTA-2006-AVI-138

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples Vulnérabilités dans les produits Cisco ONS

Gestion du document

Référence	CERTA-2006-AVI-138
Titre	Multiples Vulnérabilités dans les produits Cisco ONS
Date de la première version	06 avril 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité 05 avril 2006
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 à distance ;
- déni de service à distance.

2 Systèmes affectés

- Pour les trois premières vulnérabilités :
  - Cisco ONS 15327 Series ;
  - Cisco ONS 15454 MSPP ;
  - Cisco ONS 15454 MSTP ;
  - Cisco ONS 15600 Series ;
  - Cisco ONS 15310-CL Series.
- Pour la dernière vulnérabilité : tous les Cisco ONS de la série 15000.

3 Résumé

Plusieurs vulnérabilités dans les produits Cisco ONS permettent à un utilisateur distant de provoquer un déni de service ou d'exécuter du code arbitraire.

4 Description

Plusieurs vulnérabilités ont été identifiées dans la série 15000 des produits Cisco Optical Networking System:

- Une erreur dans la mise en œuvre de l'initialisation des connexions TCP permet à un utilisateur distant de provoquer, par le biais d'un paquet, une consommation de toute la mémoire du système vulnérable, engendrant ainsi un déni de service ;
- deux erreurs dans le traitement de certains paquets IP permettent chacune à un utilisateur distant de provoquer un déni de service ;
- une erreur dans la mise en œuvre du protocole de routage OSPF (Open Shortest Path First) permet à un utilisateur distant mal intentionné de provoquer un déni de service ;
- une vulnérabilité dans le lanceur d'*applet java* du CTC (Cisco Transport Controller) permet à un utilisateur distant mal intentionné d'exécuter du code arbitraire sur la machine utilisant ce CTC, si celle-ci est utilisée pour consulter une page web construite de façon malveillante.

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 ID 69702 du 06 avril 2006 :
  http://www.cisco.com/warp/public/707/cisco-sa-20060405-ons.shtml

Gestion détaillée du document

06 avril 2006 version initiale.