



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 22 juillet 2004
N° CERTA-2004-AVI-250

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Cisco ONS 15000

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-2004-AVI-250>

Gestion du document

Référence	CERTA-2004-AVI-250
Titre	Vulnérabilités dans Cisco ONS 15000
Date de la première version	22 juillet 2004
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco 60322
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

- Cisco ONS série 15327 (carte contrôleur XTC) ;
- Cisco ONS série 15454 (cartes contrôleur TCC/TCC+/TCC2) ;
- Cisco ONS série 15454 SDH (cartes contrôleur TCCi/TCC2) ;
- Cisco ONS série 15600 (carte contrôleur TSC).

3 Résumé

Plusieurs vulnérabilités dans les équipements de transport par fibre optique Cisco permettent à un utilisateur mal intentionné de réaliser un déni de service sur l'équipement vulnérable.

4 Description

- Une vulnérabilité référencée sous le numéro Cisco *CsCed06531* présente sur les cartes contrôleur XTC, TCC/TCC+/TCC2 et TCCi/TCC2 permet à un utilisateur mal intentionné, via l'envoi répété de paquets IP malicieusement construits, de réaliser un redémarrage des équipements vulnérables.
- Une vulnérabilité référencée sous le numéro Cisco *CsCed86946* présente sur les cartes contrôleur XTC, TCC/TCC+/TCC2 et TCCi/TCC2 permet à un utilisateur mal intentionné, via l'envoi répété de paquets ICMP malicieusement construits, de réaliser un redémarrage des équipements vulnérables.
- Une vulnérabilité référencée sous les numéros Cisco *CsCed88426*, *CsCed88508*, *CsCed85088*, *CsCeb07263*, *CsCec21429* présente sur les cartes contrôleur XTC, TCC/TCC+/TCC2, TCCi/TCC2 et XTC permet à un utilisateur mal intentionné, via l'envoi répété de paquets TCP malicieusement construits, de réaliser un redémarrage des équipements vulnérables.
Il n'y a pas d'impact sur le trafic sur les Cisco ONS série 15600 pour cette vulnérabilité, seules les fonctions de gestion de l'équipement sont impactées.
- Une vulnérabilité référencée sous les numéros Cisco *CSCec59739*, *CSCed02439*, *CSCed22547* présente sur les cartes contrôleur XTC, TCC/TCC+/TCC2 et TCCi/TCC2 permet à un utilisateur mal intentionné, par une attaque de type « TCP-ACK DOS » (envoi de paquets invalides à la place des paquets d'acquiescement pour mettre la connection TCP dans un état instable), de provoquer un redémarrage des équipements vulnérables.
- Une vulnérabilité référencée sous les numéros Cisco *CSCec88402*, *CSCed31918*, *CSCed83309*, *CSCec85982*, *CSCec21435*, *CSCee03697* présente sur les cartes contrôleur XTC, TCC/TCC+/TCC2, TCCi/TCC2 et XTC permet à un utilisateur mal intentionné, via l'envoi répété de paquets UDP malicieusement construits, de réaliser un redémarrage des équipements vulnérables.
Il n'y a pas d'impact sur le trafic sur les Cisco ONS serie 15600 pour cette vulnérabilité, seule les fonctions de gestion de l'équipement sont impactées.
- Une vulnérabilité référencée sous les numéros Cisco *CSCea16455*, *CSCea37089*, *CSCea37185* présente sur les cartes contrôleur XTC, TCC/TCC+/TCC2 et TCCi/TCC2 permet à un utilisateur mal intentionné, via l'envoi répété de paquets SNMP malicieusement construits, de réaliser un redémarrage des équipements vulnérables.
- Une vulnérabilité référencée sous le numéro Cisco *CsCee27329* présente sur l'interface d'authentification TL1 permet à un utilisateur mal intentionné de s'authentifier avec un mot de passe supérieur à dix caractères.

Ces équipements sont la plupart du temps utilisés sur un réseau local. Cela réduit l'exploitation de ces vulnérabilités depuis l'Internet.

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 60322 du 21 juillet 2004 :
<http://www.cisco.com/warp/public/707/cisco-sa-20040721-ons.shtml>

Gestion détaillée du document

22 juillet 2004 version initiale.