Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 15 juillet 2005
N° CERTA-2005-AVI-264

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans CISCO ONS 15216 OADM

Gestion du document

Référence	CERTA-2005-AVI-264
Titre	Vulnérabilité dans CISCO ONS 15216 OADM
Date de la première version	15 juillet 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité CISCO 65541 du 13 juillet 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 sur la fonctionnalité de gestion à distance.

2 Systèmes affectés

CISCO ONS 15216 OADM version 2.2.2 et versions antérieures.

3 Description

Le produit clef-en-main CISCO ONS 15216 OADM (`Optical Add/Drop Multiplexer`) permet le multiplexage de fibre optique. Il peut être administré via le service `Telnet`.

Une faille dans la gestion des sessions `Telnet` permettrait à un utilisateur mal intentionné, après avoir ouvert une session (ce qui nécessite une authentification préalable), de causer un déni de service via certaines requêtes habilement construites.

Le déni de service n'impacte que le service d'administration à distance, et le trafic n'est en rien perturbé par une telle attaque. En revanche, un redémarrage de la machine est necessaire pour réactiver le service d'administration, ce qui provoque une interruption du trafic.

4 Solution

Utiliser CISCO ONS 15216 OADM version 2.2.3

5 Documentation

– Bulletin de sécurité CISCO 65541 du 13 juillet 2005
http://www.cisco.com/warp/public/707/cisco-sa-20050713-ons.shtml

Gestion détaillée du document

15 juillet 2005 version initiale.