Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 20 août 2004
N° CERTA-2004-AVI-273

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du système d'exploitation Cisco IOS

Gestion du document

Référence	CERTA-2004-AVI-273
Titre	Vulnérabilité du système d'exploitation Cisco IOS
Date de la première version	20 août 2004
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco #61365 du 18 août 2004
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 IOS versions 12.0S, 12.2 et 12.3.
Les versions Cisco IOS 12.1, 12.0 et antérieures ne sont pas affectées.

3 Résumé

Une vulnérabilité dans la gestion du protocole OSPF par le systèmes d'exploitation Cisco IOS permet à un utilisateur distant mal intentionné de provoquer un déni de service.

4 Description

OSPF (Open Shortest Path First) est un protocole de routage.

Une vulnérabilité a été découverte dans la gestion de ce protocole par le système d'exploitation IOS de certains équipements Cisco.

Elle permet à un utilisateur mal intentionné de provoquer un déni de service par le biais d'un paquet OSPF malicieusement construit.

5 Contournement provisoire

- Utiliser l'authentification OSPF (cf. section Documentation) ;
- Utiliser des listes de contrôle d'accès (ACLs) pour protéger le réseau (cf. section Documentation).

6 Solution

Appliquer le correctif proposé par Cisco (cf. section Documentation).

7 Documentation

- Bulletin de sécurité Cisco #61635 du 18 août 2004 :
  http://www.cisco.com/warp/public/707/cisco-sa-20040818-ospf.shtml
- Informations sur l'authentification OSPF :
  http://www.cisco.com/warp/public/104/25.shtml
- Informations sur les listes de contrôle d'accès :
  http://www.cisco.com/warp/public/707/iacl.html

Gestion détaillée du document

20 août 2004 version initiale.