



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 10 août 2007
N° CERTA-2007-AVI-350

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Cisco IOS

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-2007-AVI-350>

Gestion du document

Référence	CERTA-2007-AVI-350
Titre	Multiples vulnérabilités dans Cisco IOS
Date de la première version	10 août 2007
Date de la dernière version	–
Source(s)	Bulletins de sécurité Cisco du 08 août 2007
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 ;
- atteinte à la confidentialité des données ;
- contournement de la politique de sécurité.

2 Systèmes affectés

- Cisco IOS 12.x ;
- Cisco IOS R12.x ;
- Cisco IOS XR 3.x ;
- Cisco Unified Communications Manager.

3 Résumé

De multiples vulnérabilités affectent différentes versions de Cisco IOS et permettent notamment d'exécuter du code arbitraire à distance.

4 Description

Plusieurs vulnérabilités affectent Cisco IOS :

- la première (cisco-sa-20070808-scp), affectant l'implémentation de Secure Copy (SCP), permet à un utilisateur connecté localement de contourner la politique de sécurité ;
- la seconde (cisco-sa-20070808-nhrp), présente dans le protocole Next Hop Resolution Protocol (NHRP), permet à un utilisateur distant malintentionné de réaliser un déni de service ou d'exécuter du code arbitraire par le biais d'un paquet spécialement conçu ;
- la troisième (cisco-sa-20070808-IOS-IPv6-leak) permet à un utilisateur distant de réaliser un déni de service ou de porter atteinte à la confidentialité des données par le biais d'un paquet IPv6 malicieusement construit ;
- les dernières (cisco-sa-20070808-IOS-voice) concernent également le produit Cisco Unified Communications Manager. Ces vulnérabilités affectent les protocoles Session Initiation Protocol (SIP), Media Gateway Control Protocol (MGCP), H.323, H.254, Real-time Transport Protocol (RTP) et Facsimile reception. Un utilisateur distant exploitant ces vulnérabilités peut réaliser un déni de service ou exécuter du code arbitraire par le biais d'un paquet malicieusement construit.

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 cisco-sa-20070808-scp du 08 août 2007 :
<http://www.cisco.com/warp/public/707/cisco-sa-20070808-scp.shtml>
- Bulletin de sécurité Cisco cisco-sa-20070808-nhrp du 08 août 2007 :
<http://www.cisco.com/warp/public/707/cisco-sa-20070808-nhrp.shtml>
- Bulletin de sécurité Cisco cisco-sa-20070808-IOS-IPv6-leak du 08 août 2007 :
<http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-IPv6-leak.shtml>
- Bulletin de sécurité Cisco cisco-sa-20070808-IOS-voice du 08 août 2007 :
<http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml>
- Référence CVE CVE-2007-4263 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4263>

Gestion détaillée du document

10 août 2007 version initiale.