Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 27 mars 2008
N° CERTA-2008-AVI-163

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Cisco IOS

Gestion du document

Référence	CERTA-2008-AVI-163
Titre	Multiples vulnérabilités dans Cisco IOS
Date de la première version	27 mars 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco 100893 du 26 mars 2008
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 à distance ;
- contournement de la politique de sécurité ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

Les `Cisco IOS` déployés sont vulnérables dans les cas suivants :
- les versions antérieures à la 12.3 avec le `VPDN` (*Virtual Private Dial-up Network*) activé ;
- les versions antérieures à la 12.3 avec le `DLSw` (*Data Link Switching*) activé ;
- certaines versions antérieures à la 12.3 avec le support IPv6 activé ainsi que l'UDP en IPv4 ;
- certaines versions antérieures à la 12.3 avec le `MVPN` (*Multicast Virtual Private Network*) activé ;
- certaines sous-versions de la 12.2 équipant les *Cisco Catalyst 6500* et *Cisco 7600 router*, configurées avec `OSPF` (*Open Shortest Path First*) et `MPLS VPN` (*Multi Protocol Label Switching Virtual Private Networking*).

3 Résumé

Cisco a publié un bulletin de sécurité regroupant cinq bulletins sur des vulnérabilités séparées. Elles concernent toutes `Cisco IOS` et plus précisément `PPTP`, `DLSw`, `IPv6`, `MVPN` et `MPLS VPN`.

4 Description

`Cisco IOS` (*Internetwork Operating System*) est le système d'exploitation de la majorité des routeurs et commutateurs Cisco.

- `PPTP` : des vulnérabilités concernant une fuite de mémoire et une mauvaise gestion des blocs décrivant les interfaces permettent un épuisement des ressources entrainant un déni de service.
- `DLSw` : une vulnérabilité affectant le traitement des trames UDP et IP (protocole 91) permet un redémarrage ou un déni de service à distance par épuisement des ressources mémoire.
- `IPv6` : une vulnérabilité permet à l'aide d'une trame IPv6, spécifiquement créée et ciblant un équipement, de provoquer un déni de service de l'interface ou de l'équipement en fonction des cas.
- `MVPN` : une trame `MDT` (*Multicast Distribution Tree*) spécifiquement créée permet de détourner une partie du trafic du réseau virtuel privé.
- `MPLS VPN` : une vulnérabilité permet le blocage des files, des fuites mémoire et le redémarrage de l'équipement.

5 Solution

Se référer au bulletin de sécurité Cisco 100893 du 26 mars 2008 pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Cisco 20080326-bundle du 26 mars 2008 :
  http://www.cisco.com/warp/public/707/cisco-sa-20080326-bundle.shtml
- Bulletin de sécurité Cisco 20080326-pptp du 26 mars 2008 :
  http://www.cisco.com/warp/public/707/cisco-sa-20080326-pptp.shtml
- Bulletin de sécurité Cisco 20080326-dlsw du 26 mars 2008 :
  http://www.cisco.com/warp/public/707/cisco-sa-20080326-dlsw.shtml
- Bulletin de sécurité Cisco 20080326-IPv4IPv6 du 26 mars 2008 :
  http://www.cisco.com/warp/public/707/cisco-sa-20080326-IPv4IPv6.shtml
- Bulletin de sécurité Cisco 20080326-mvpn du 26 mars 2008 :
  http://www.cisco.com/warp/public/707/cisco-sa-20080326-mvpn.shtml
- Bulletin de sécurité Cisco 20080326-queue du 26 mars 2008 :
  http://www.cisco.com/warp/public/707/cisco-sa-20080326-queue.shtml
- Référence CVE CVE-2008-0537 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0537
- Référence CVE CVE-2008-1150 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1150
- Référence CVE CVE-2008-1151 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1151
- Référence CVE CVE-2008-1152 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1152
- Référence CVE CVE-2008-1153 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1153
- Référence CVE CVE-2008-1156 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1156

Gestion détaillée du document

27 mars 2008 version initiale.