Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 30 août 2004
N° CERTA-2004-ALE-010

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilité du service Telnet de Cisco IOS

Gestion du document

Référence	CERTA-2004-ALE-010
Titre	Vulnérabilité du service Telnet de Cisco IOS
Date de la première version	30 août 2004
Date de la dernière version	–
Source(s)	Bulletin de sécurité Cisco du 27 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

Toutes les versions du système d'exploitation Cisco IOS.

3 Résumé

Une vulnérabilité du service *telnet* (et *reverse telnet*) du système d'exploitation Cisco IOS permet à un utilisateur distant de provoquer un déni de service.

4 Description

Une vulnérabilité a été découverte dans la gestion des paquets TCP des services *telnet* et *reverse telnet* par le système d'exploitation Cisco IOS.

Le service *telnet* (port 23/tcp) est utilisé pour l'administration des équipements sous Cisco IOS.

Le service *reverse telnet* est utilisé pour se connecter à un équipement tiers via une connexion *telnet* vers un équipement Cisco. Ce service utilise les ports suivants :

- 2001/tcp à 2999/tcp ;
- 3001/tcp à 3099/tcp ;
- 6001/tcp à 6999 /tcp ;
- 7001/tcp à 7099/tcp.

La vulnérabilité peut être exploitée par l'envoi d'un paquet TCP malicieusement construit à destination du port 23 ou de l'un des ports du service *reverse telnet*.

Un utilisateur distant mal intentionné peut utiliser cette vulnérabilité pour provoquer un déni de service des services d'administration *telnet*, *reverse telnet*, *RSH* (port 514/tcp), *SSH* (port 22/tcp), *SCP* (port 22/tcp) et dans certains cas *HTTP* (port 80/tcp).

Les autres services (routage des paquets, protocoles de routage, ...) ne sont pas affectés. De plus, les connexions des services d'administration établies avant une attaque restent actives après celle-ci.

5 Contournement provisoire

- Activer le service *SSH* et désactiver le service *telnet* (cf. section Documentation) ;
- établir des classes d'accès sur les terminaux virtuels VTY (cf. section Documentation) ;
- établir des listes de contrôles d'accès (cf. section Documentation).

6 Solution

Cisco n'a pas encore publié de correctif pour cette vulnérabilité.

7 Documentation

- Bulletin de sécurité Cisco du 27 août 2004 :
  http://www.cisco.com/warp/public/707/cisco-sa-20040827-telnet.shtml
- Activation du service *SSH* :
  http://cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca7d5.html#100116

- Etablissement des classes d'accès sur les terminaux virtuels VTY :
  http://cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_reference_chapter09186a00800873c8.html#wp101

- Etablissement des listes d'accès *Transit ACL*:
  http://www.cisco.com/warp/public/707/tacl.html
- Etablissement des listes d'accès *Infrastructure ACL*:
  http://www.cisco.com/warp/public/707/iacl.html
- Etablissement des listes d'accès *Receive ACL*:
  http://www.cisco.com/warp/public/707/racl.html

Gestion détaillée du document

30 août 2004 version initiale.