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 avril 2001
N° CERTA-2001-AVI-047

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans IPTables sous linux 2.4

Gestion du document

Référence	CERTA-2001-AVI-047
Titre	Vulnérabilité dans IPTables sous linux 2.4
Date de la première version	27 avril 2001
Date de la dernière version	–
Source(s)	RHSA-2001:052-02
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

Contournement des règles de filtrage de IPTables.

2 Systèmes affectés

Tout système linux avec un des noyaux suivants:
- kernel 2.4.3 ;
- kernel 2.4.2 ;
- kernel 2.4.1 ;
- kernel 2.4.0-test1 ;
- kernel 2.4.

3 Résumé

IPTables est un des composants utilisé pour le filtrage des paquets réseaux.

Une erreur dans l'implémentation de IPTables permet à un attaquant de contourner les règles de filtrage mises en oeuvre par un pare-feu utilisant IPTables.

Ce contournement est possible dans le cas de connexions FTP marquées « `related` ».

4 Description

Avec IPTables, une règle de filtrage utilisant le mot clef « `related` » s'appliquera à un paquet initialisant une nouvelle connexion qui est en relation avec une connexion existante.

Le module `ip_conntrack_ftp` est chargé d'ajouter les connexions FTP définies par les commandes `PORT` et `PASV` à la table des connexions autorisées.

Le module `ip_conntrack_ftp` n'analysant pas correctement les paramètres de la commande `PORT`, un attaquant peut envoyer des paquets FTP à un serveur (à travers le pare-feu) en utilisant des adresses ip et ports tcp arbitraires afin d'ouvrir des trous dans le filtrage du pare-feu (ouvrir des ports normalement fermés conformément à la politique de sécurité en vigueur sur le site protégé par le pare-feu).

5 Contournement provisoire

Ne pas utiliser les connexions FTP « `related` ».

6 Solution

- Un correctif est disponible :
  http://netfilter.samba.org/security-fix/ftp-security2.patch
- RedHat 7.1 est livrée avec le module `ip_conntrack_ftp` incriminé mais n'utilise pas par défaut IPTables.
  http://www.redhat.com/support/errata/RHSA-2001-052.html

7 Documentation

Avis RedHat RHSA-2001:052-02
http://www.redhat.com/support/errata/RHSA-2001-052.html

Gestion détaillée du document

27 avril 2001 version initiale.