



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 15 mai 2002
N° CERTA-2002-AVI-100

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité sur Netfilter (iptables)

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-2002-AVI-100>

Gestion du document

Référence	CERTA-2002-AVI-100
Titre	Vulnérabilité sur Netfilter (iptables)
Date de la première version	15 mai 2002
Date de la dernière version	–
Source(s)	Bulletin de sécurité 20020402 de CARTEL
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

Divulgateion d'informations sur la topologie du réseau.

2 Systèmes affectés

Versions iptables antérieures à la version 1.2.6a.

3 Résumé

Une vulnérabilité présente dans l'implémentation de iptables permet à un utilisateur mal intentionné de retrouver la topologie d'un réseau local si la traduction d'adresses est utilisée.

4 Description

iptables est un des composants utilisés pour le filtrage des paquets réseau sur les noyaux Linux supérieurs à la version 2.4.x. Ce garde barrière permet également d'effectuer de la traduction d'adresses (NAT) vers un réseau local.

Un utilisateur mal intentionné peut, par le biais de paquets malicieusement construits, provoquer des messages d'erreurs ICMP. Ces messages d'erreurs peuvent contenir les adresses IP des machines du réseau interne, accompagnées des ports en écoute sur ces machines.

5 Contournement provisoire

Il n'existe pas de correctif disponible pour le moment, cependant il est possible de contourner le problème en appliquant la règle de filtrage suivante :

```
iptables -A OUTPUT -m state -p icmp -state INVALID -j DROP
```

6 Documentation

- Bulletin de sécurité 20020402 de Cartel :
<http://netfilter.samba.org/security/2002-04-02-icmp-dnat.html>
- Bulletin de sécurité MDKSA-2002:030 de Mandrake :
<http://www.mandrakesecure.net/en/advisories/2002/MDKSA-2002-030.php>
- Bulletin de sécurité RHSA-2002:086 de Redhat :
<http://rhn.redhat.com/errata/RHSA-2002-086.html>

Gestion détaillée du document

15 mai 2002 version initiale.