Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 23 mai 2006
N° CERTA-2006-AVI-212-001

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité des routeurs Linksys WRT54G

Gestion du document

Référence	CERTA-2006-AVI-212-001
Titre	Vulnérabilité des routeurs Linksys WRT54G
Date de la première version	23 mai 2006
Date de la dernière version	24 mai 2006
Source(s)	Mise à jour de Linksys du 16 mai 2006
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 de la politique de sécurité.

2 Systèmes affectés

Toutes les versions du logiciel matériel (ou *firmware*) pour les routeurs Linksys WRT54G Wireless-G Broadband antérieures à 1.00.9.

3 Résumé

Une vulnérabilité a été identifiée dans le logiciel de fonctionnement des routeurs Linksys WRT54G Wireless-G Broadband. Elle peut être utilisée par une personne malveillante pour rediriger du trafic à partir du réseau local vers une machine distante, et ainsi contourner la politique de sécurité en vigueur.

4 Description

Une vulnérabilité a été identifiée dans le logiciel de fonctionnement (*firmware*) des routeurs Linksys WRT54G Wireless-G Broadband. Il n'authentifie pas de manière correcte certaines requêtes UPnP (pour *Universal Plug &*

Play) de type `AddPortMapping` : la validation du champ `InternalClient` de la requête ne se fait pas. Un utilisateur malveillant peut profiter de cette vulnérabilité pour configurer le transfert de ports (ou *port forwarding*) et diriger le trafic issu d'une machine locale vers une autre machine à l'extérieur du réseau. La politique de sécurité est alors contournée.

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation). Le correctif français n'existe pas encore. Il est fortement recommandé de désactiver le protocole UPnP si celui-ci n'est pas utilisé. Pour cela, se reporter au manuel de l'utilisateur qui indique comment décocher l'option `UPnP` dans l'interface web d'administration.

6 Documentation

Bulletin de mise à jour Linksys du 16 mai 2006 :
http://www.linksys.com/download/

Gestion détaillée du document

23 mai 2006 version initiale.
24 mai 2006 ajout d'un contournement provisoire pour la version française.