Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 18 juillet 2006
N° CERTA-2006-AVI-297

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité sur les routeurs D-Link

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-2006-AVI-297

Gestion du document

Référence	CERTA-2006-AVI-297
Titre	Vulnérabilité sur les routeurs D-Link
Date de la première version	18 juillet 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité eeye
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

- Exécution de code arbitraire à distance ;
- déni de service à distance ;
- contournement de la politique de sécurité.

2 Systèmes affectés

- D-Link DI-254 ;
- D-Link DI-604 Broadband Router ;
- D-Link DI-624 ;
- D-LINK EBR-2310 Ethernet Broadband Router ;
- D-Link WBR-1310 Wireless G Router ;
- D-Link WBR-2310 RangeBooster G Router.

3 Résumé

Une vulnérabilité présente sur les routeurs D-Link peut être exploitée par un utilisateur mal intentionné pour exécuter du code arbitraire sur les appareils vulnérables.

4 Description

Une vulnérabilité de type débordement de mémoire est présente dans le taritement des requêtes *"M-Search"* du service *UPnP*. Un utilisateur mal intentionné peut exploiter cette vulnérabilité et exécuter du code arbitraire sur les appareils vulnérables via l'envoi d'une requête spécialement construite.

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité eEye :
  http://www.eeye.com/html/research/advisories/AD20060714.html
- Site internet de D-Link :
  http://www.dlink.com

Gestion détaillée du document

18 juillet 2006 version initiale.