

# Des routeurs D-Link affectés par une grave faille de sécurité

Bien que les routeurs concernés ne soient pas commercialisés en Europe, la nouvelle est désormais connue. Certains routeurs de la marque D-Link sont affectés par une faille. Les modèles DI-524 C1, DIR-628 B2 et DIR-655 A1 en vente depuis 2006 sont touchés par une « **grave faille** » selon les spécialistes.

A en croire le site *SourceSec*, les trois modèles concernés seraient donc vulnérable aux attaques de *hackers*. La faute du protocole d'administration au niveau de l'identification des utilisateurs et administrateurs. Il serait donc possible d'exploiter cette faille pour **accéder aux paramètres réseau** et donc s'y introduire que ce soit en local ou de l'extérieur. Plus précisément, cette vulnérabilité toucherait le protocole HNAP (Home Network Administration Protocol) qui permet d'améliorer l'authentification des utilisateurs avec un code Capcha. Des attaquants locaux et externes pourraient alors exploiter la faille afin d'accéder aux paramètres réseau du routeur.

Bien qu'avertie du phénomène, la société D-Link a expliqué que les produits encore vendus en Asie et en Amérique du Nord ne seront pas automatiquement remplacés. Des **correctifs devraient ainsi arriver d'ici peu** même si aucune date n'a encore été avancée. Pour autant, les questions de protection de la technologie Captcha sont presque une alésienne chez D-Link.

Déjà, le système d'**authentification des systèmes d'administration** avait fait l'actualité des sites de hacking en mai dernier. Certains pirates avaient réussi à trouver des failles permettant de craquer une clé WPA et de s'infiltrer sur des réseaux sans-fil.

De même, une autre **faille de sécurité concernant la gestion UPnP** (Universal Plug and Play) avait touché sept produits (dont le DI-524, encore concerné aujourd'hui) au mois de février 2006. Après ces déboires, D-Link va devoir établir de nouvelles règles de sécurité pour ses produits. Une sorte de guide du routeur.