Check Point ressort son arme contre les attaques 'RPC'

Mieux vaut un peu plus tard que jamais… Check Point présente -ou plutôt réactualise SmartDefense: ce serait l'antidote pour protéger les clients contre les failles découvertes ou redécouvertes récemment.

Des pirates ont montré qu'ils pouvaient exploiter des failles dans les appels de procédures à distance ou RPC, technique utilisée dans les architectures client/serveur depuis des années et permettant de lancer des requêtes de ressources 'système' à distance. D'où la tentation des « hackers » d'en détourner l'utilisation. Check Point rappelle que sa première mise à jour, qui date d'avril dernier, a protégé les clients contre certaines variantes de virus exploitant déjà ce mode RPC de Microsoft, y compris le ver LovSan/Blaster réapparu en juillet. La protection préconisée par Check Point repose sur ses technologies Stateful Inspection et Application Intelligence conçues pour bloquer de telles attaques, sans se fier aux signatures (qui peuvent être usurpées). L'une des parades consiste donc à déterminer si les données internes aux protocoles respectent l'utilisation attendue: « *Si un flux de communication respecte un standard de protocole, la manière dont le protocole est utilisé peut se révéler incohérente avec ce qui en est attendu* », explique-t-on chez Check Point. L'utilisation du FireWall-1 NG, et du Feature Pack 3 associé, permettrait une « *défense proactive*« .