Une attaque Web plante les IPS de Tipping Point

« La société a découvert le problème vendredi et a aussitôt apporté les modifications adéquates au logiciel TOS (Tippint Point OS) quelques heures plus tard », explique Laura Craddick, responsable des relations presse de Tipping Point. *« Un bug dans le moteur Tipping Point a induit une charge élevée de la CPU chez quelques-uns de nos clients utilisant des appliances en frontal d'Internet »*, poursuit Laura Craddick. *« Le bug affecte TOS 2.1 et 2.2 »*. Et l'université York de Toronto en a fait les frais. *« Vendredi 13 (NdT !), nos appliances Tipping Point ont commencé a rebooter de manière répétitive »*, explique Ramon Kagan, de l'équipe sécurité et réseaux de l'Université. *« Le crash a été provoqué par un flux HTTP qui ciblait une vulnérabilité sur un produit tiers »*. Nous n'en saurons malheureusement pas plus. Il est intéressant de relever que cet incident est survenu un jour après que Tipping Point ait fourni une mise à jour des signatures, ce qui a d'ailleurs animé certains forums de discussion tenus par les utilisateurs de Unity One. Même la vénérable liste SF-IDS de SecurityFocus vient d'initier un débat sur la qualité des signatures au sein des IPS (sans citer de nom de produits. (Voir http://www.securityfocus.com/archive/96/422264/30/0/threaded) Laura Craddick soutient néanmoins que le problème est dû à une faille logicielle, et non à une mauvaise signature. Bien que l'incident ait eu un impact non neutre pour les équipes d'exploitation de l'Université de York, Ramon Kagan se dit toutefois très satisfait de la réactivité du constructeur, qui a fourni un patch dans un délai de cinq heures. Les clients Tipping Point en version 2.1.4.6324 ont été invités à mettre à jour au plus vite leurs appliances vers la version 2.2.1.6506.