

Alerte : découverte d'une vulnérabilité dans le navigateur de l'iPhone

Le fournisseur de solutions intégrées de distribution d'applications pour les réseaux orientés métier, Radware, annonce que l'équipe de recherche spécialisée de son centre de sécurité opérationnelle a découvert une vulnérabilité de type déni de service (*denial of service*, ou DoS) dans le navigateur Safari de l'iPhone version 1.1.4 d'Apple.

Une protection immédiate est disponible dans le cadre du service des mises à jour de sécurité de Radware, pour préserver les infrastructures des clients avant la divulgation publique de la faille.

Pour être victime de cette faille, l'utilisateur d'un iPhone doit ouvrir une page HTML contenant du code JavaScript qui contient l'attaque.

La divulgation de cette page peut être due à un campagne d'ingénierie sociale (par exemple, e-mail ou SMS de spam). L'utilisateur est alors confronté à un déni de service au niveau applicatif qui se traduit par un plantage du navigateur Safari et qui peut même aboutir à un arrêt complet de l'appareil iPhone.

Itzik Kotler, directeur du centre de sécurité opérationnelle de Radware, estime que *« dans leur course pour lancer de nouveaux produits et applications, les fournisseurs négligent de toute évidence la priorité que doit être la sécurité. Les pirates continuent à détourner les logiciels d'autres personnes et leur tâche s'avère facilitée par des failles de conception que ces produits intègrent. »*

Le navigateur iPhone Safari d'Apple est vulnérable à des attaques DoS en raison d'une faille de conception.

Cette dernière peut être exploitée suite à une série d'opérations d'allocation dans le 'pool' de mémoire dynamique, ce qui peut déclencher un 'bug' dans le gestionnaire de corbeille.

Aucun correctif n'existe actuellement pour cette faille de sécurité; les propriétaires d'iPhone restent donc vulnérables face à de possibles attaques tant qu'Apple ne publie pas une mise à jour de sécurité.