Bee Ware : anticipe les menaces liÃ©es Ã l'utilisation d'HTML5
Internet
PostÃ© par : JPilo
PubliÃ©e le : 30/11/2012 13:00:00

Dans son Ã©tude "**Hype Cycle for Web Computing 2012**",datant du 1er aoÃ»t 2012, le Gartner annonce l'utilisation du langage HTML5 par l'ensemble de la population pour 2017.

Cette prÃ©diction, due essentiellement Ã l'essor de la mobilitÃ©, soulÃ¨ve par ailleurs de nouvelles problÃ©matiques sÃ©curitaires. Pour faire face Ã ces menaces, le Gartner recommande d'utiliser dÃ¨s Ã prÃ©sent des mesures de protection adaptÃ©es.

Prochaine rÃ©vision majeure du format de donnÃ©es HTML, le langage HTML5 est en cours d'Ã©laboration depuis maintenant plusieurs annÃ©es. Le W3C* et le WHATWG** travaillent conjointement aux spÃ©cifications de ce langage, dont la finalitÃ© sera d'offrir aux applications web toujours plus de dynamisme et de qualitÃ©.

Bien que la finalisation des spÃ©cifications de ce langage ne soit officiellement prÃ©vue qu'en 2014, le W3C encourage dÃ¨s Ã prÃ©sent son utilisation afin d'en amÃ©liorer l'usage.

TrÃ¨s vite adoptÃ© par les dÃ©veloppeurs d'applications Web, HTML5 connait un succÃ¨s grandissant, principalement dÃ» au fait qu'il permet de reproduire les caractÃ©ristiques habituellement proposÃ©es par les logiciels propriÃ©taires (i.e. Flash, Silverlight, etc.).

Au programme des Ã©volutions proposÃ©es, on notera particuliÃ¨rement :

â¢ Une mise en forme simplifiÃ©e et standardisÃ©e des pages Web

â¢ L'optimisation de l'affichage selon la taille de l'Ã©cran

â¢ L'intÃ©gration de pistes audio et vidÃ©o sans technologie tierce

â¢ Un stockage interne permettant de profiter de certaines applications web en mode "hors connexion"

â¢ De nouvelles balises supportant la gestion de nombreux Ã©vÃ¨nements Client

â¢ Etc.

Outre le dÃ©veloppement aisÃ© de sites Web et d'applications mobiles, l'utilisation prÃ©coce d'HTML5 a Ã©galement permis de mettre en Ã©vidence de nombreuses failles de sÃ©curitÃ©...

En effet, les systÃ¨mes actuels de protection n'Ã©tant pas prÃ©parÃ©s aux nouvelles fonctionnalitÃ©s proposÃ©es (et donc aux nouvelles structures syntaxiques), l'utilisation d'HTML5 a mis en Ã©vidence de nouvelles vulnÃ©rabilitÃ©s.

De nombreuses recherches menÃ©es sur le sujet ont fait ressortir les possibilitÃ©s d'attaques suivantes :

â¢ CÃ´tÃ© client

o L'injection de code malicieux ou de librairies corrompues dans le Cache Manifest (cache permettant aux applications de fonctionner hors ligne)

o Le Filejacking, vol de fichiers utilisant la balise file directory de l'API fichiers de HTML5

o L'accÃ¨s non autorisÃ© aux microphones, webcams et autres outils de gÃ©olocalisation

o La rÃ©cupÃ©ration de donnÃ©es sensibles (login, mot de passe, etc.) via les espaces de stockage local d'HTML5 (espaces mis Ã disposition des applications Web)

â¢ CÃ´tÃ© serveur

o La reviviscence d'attaques, telles les "cross-site requests", "cross-site scirpting" ou "html injection".

Pour rÃ©pondre Ã ces nouvelles menaces, Bee Ware a dÃ©veloppÃ© une mise Ã jour complÃ©tant les rÃ¨gles de filtrage de la plate-forme de sÃ©curitÃ© i-Suite.

L'ensemble des produits Bee Ware sont donc dÃ©sormais protÃ©gÃ©s contre toute tentative visant Ã contourner, via les nouveaux Ã©lÃ©ments HTML5, les protections d'ores et dÃ©jÃ mises en place.