



rWeb v4: Une nouvelle version aux multiples innovations

Par Ludovic Blin, secuobs.com
Le 26/01/2010

Résumé : La nouvelle version du produit de sécurisation des applications web, xml et ftp de l'éditeur français Deny All est enrichie de nombreuses nouvelles fonctions: haute disponibilité actif/actif, nouvelle interface Ajax, protection du poste client, des services web, API de configuration, fonctions DLP ...

Face au nombre très important et sans cesse croissant d'attaques touchant les applications web, ainsi qu'aux exigences réglementaires croissantes, de nombreuses organisations font le choix de protéger leurs applications par un dispositif indépendant de type WAF (Web Application Firewall) fonctionnant comme un reverse-proxy. En effet, cette solution offre l'avantage d'apporter une réponse unique avec un déploiement rapide au besoin de sécurisation d'une ou plusieurs applications web.

L'éditeur français Deny All, qui est spécialisé dans le domaine des WAF depuis plus de 10 ans, a annoncé la sortie de la nouvelle version de son produit phare, rWeb. Ce dernier est utilisé depuis longtemps par de nombreuses entreprises, notamment dans le secteur financier.

« rWeb v4 bénéficie du retour d'expérience de nos clients depuis plus de 10 ans et intègre de nombreuses innovations, destinées aussi bien à augmenter la sécurité des applications protégées, qu'à optimiser la mise en place et l'exploitation du produit. » déclare Renaud Bidou, directeur technique de Deny All.

Le produit intègre ainsi une liste étendue de fonctions de sécurité et de filtrage: analyse « stateful », liste blanche, liste noire, scoring list, analyse comportementale, prévention des fuites de données, sécurisation du poste client, protection des services web, prévention des attaques DoS (notamment slowloris), fonctionnement en mode pooling, anti-évasion ...

Plusieurs de ces fonctions sont habituelles des produits du marché, mais certaines sont uniques à rWeb, comme par exemple le fonctionnement en mode pooling permettant une communication unidirectionnelle entre une DMZ externe et une DMZ interne hébergeant les applications. Le système de scoring list permet quant à lui de filtrer les requêtes en fonction de différents critères d'importance variable et donc de se protéger contre des attaques inconnues. Le choix de ces critères et de leurs poids est issu de l'expérience accumulée par les nombreux environnements dans lesquels le produit est déployé. Le module « client sanitization » est pour sa part destiné à assurer une isolation entre le navigateur utilisé pour l'application protégée, et les autres fenêtres ou onglets de l'utilisateur.

La protection des services web est aussi une fonction particulièrement intéressante vu leur déploiement croissant et le manque de sécurité habituel des infrastructures associées.

« La demande de sécurisation des services web est très importante actuellement » confirme Renaud Bidou.

Pour cette nouvelle version, l'accent a été également mis sur l'optimisation de l'installation, de la configuration et du déploiement. Ainsi, l'interface d'administration a été complètement refaite, et utilise désormais les technologies AJAX. Elle est dotée d'une aide contextuelle très pratique et offre différents niveaux de configuration, permettant aussi bien d'avoir une vue générale des politiques de sécurité que de modifier finement un paramètre de l'une d'entre elles. Les « best practices » sont configurées par défaut. Il est possible de rajouter rapidement des exceptions aux politiques pour traiter les problèmes de faux positifs, et des fonctions de reporting et monitoring avancées sont incluses.

Une API SOAP ouverte permet désormais également au client de développer sa propre interface de configuration, en fonction de ses besoins.

L'architecture de la solution a aussi été revue. Il est ainsi possible de décomposer ses fonctions en une dizaine de modules, qui peuvent être installés sur des machines séparées (ou des clusters de taille variable). La haute disponibilité est désormais assurée en mode actif/actif, avec une latence de basculement de moins d'une seconde.

Au final cette nouvelle version de rWeb semble particulièrement solide et dotée d'un éventail de fonctions très large, certaines étant uniques à ce produit. L'approche retenue par la société, qui consiste à tirer partie au maximum de l'expérience et des demandes de ses clients, paraît aussi pertinente. Les nombreuses fonctions présentes permettent de mettre en place une défense en profondeur, qui assure de plusieurs manières différentes la sécurité des applications.

Le site de Deny All : [lien](#)