Hardware : Boitiers FortiWeb, Pare-Feux Applicatifs Web
Hardware
PostÃ© par : JPilo
PubliÃ©e le : 3/2/2011 11:00:00

Fortinet lâ□□un des principaux acteurs du marchÃ© de la sÃ©curitÃ© rÃ©seau et le leader mondial des systÃ¨mes unifiÃ©s de sÃ©curitÃ© UTM (unified threat management) â□□ annonce un changement majeur du **firmware des boitiers de pare-feux applicatifs web FortiWebâ□¢.**

Les appliances FortiWeb fournissent aux clients Grands Comptes, fournisseurs de services applicatifs, de sÃ©curitÃ© informatique externalisÃ©e (SaaS) et de services d'infogÃ©rance en sÃ©curitÃ© (MSSP) des capacitÃ©s de sÃ©curitÃ© considÃ©rablement Ã©tendues visant Ã renforcer et simplifier la protection des applications Web sensibles, contenant des donnÃ©es rÃ©glementÃ©es et confidentielles.

Le firmware FortiWeb 4.0 MR2 apporte dâ□□importantes amÃ©liorations dont des solutions de protection Ã©tendue contre les attaques aidant les organisations Ã atteindre et maintenir plus facilement la conformitÃ© aux normes de sÃ©curitÃ© informatique des donnÃ©es de lâ□□industrie des cartes de paiement (PCI DSS 6.6) et prÃ©venant du vol dâ□□identitÃ©, de la fraude financiÃ¨re et de lâ□□espionnage industriel associÃ© aux applications web stratÃ©giques.

La gamme des appliances FortiWeb dâ□□applications web et de pare-feux XML intÃ©grÃ©s offre une protection multi-couches et spÃ©cifique contre les menaces visant les applications. Ces appliances consolident de faÃ§on unique les fonctions de pare-feu dâ□□applications Web, de filtrage XML, dâ□□accÃ©lÃ©ration de trafic web et dâ□□Ã©quilibrage de trafic dâ□□applications dans un seul appareil. EquipÃ© dâ□□un firmware FortiWeb 4.0 MR2, les appliances FortiWeb tirent profit de techniques avancÃ©es pour assurer une protection bi-directionnelle contre les menaces sophistiquÃ©es comme les injections SQL et les attaques de type cross-site scripting. Un nouveau Scanner des VulnÃ©rabilitÃ©s Web est Ã©galement offert pour fournir une couche additionnelle de visibilitÃ© pour dÃ©tecter les vulnÃ©rabilitÃ©s existantes ciblant les applications web spÃ©cifiques.

Cette fonction est primordiale pour atteindre et maintenir la conformitÃ© des plus rÃ©centes spÃ©cifications du PCI DSS 6.5 et 6.6 visant Ã sÃ©curiser les applications web qui traitent, stockent ou transmettent les donnÃ©es des cartes de paiement. Ces spÃ©cifications exigent des pare-feux applicatifs web et des capacitÃ©s dâ□□Ã©valuation des vulnÃ©rabilitÃ©s, qui sont fournis par Fortinet dans un seul appareil.

Â« *Les nouvelles vulnÃ©rabilitÃ©s sont persistantes, et quand on y ajoute la complexitÃ© des*

dÃ©fis continuels de patching et des rÃ©visions de code, nous avons constatÃ© que la protection multi-couches de lâappliance FortiWeb pouvait pro-activement et efficacement protÃ©ger les applications Web et les informations associÃ©es contre les attaques et les pertes de donnÃ©es Â», dÃ©clare **le Capitaine IngÃ©nieur Antonio Ianniello**, chef de la section du dÃ©veloppement des applications et de l'expÃ©rimentation chez Aeronautica Militare.

Avec le nouveau firmware FortiWeb 4.0 MR2, les appliances FortiWeb sont dotÃ©es de fonctions de sÃ©curitÃ© et dâutilisation supplÃ©mentaires qui incluent :

â¢ Une protection robuste contre les attaques dâinclusion de fichiers Ã distance

â¢ Des restrictions de tÃ©lÃ©chargements de fichiers qui contrÃ´lent dorÃ©navant quels types de fichiers (jpg, exe, zip, etc) peuvent Ãªtre tÃ©lÃ©chargÃ©s Ã partir des applications web

â¢ Des amÃ©liorations de prÃ©vention des pertes de donnÃ©es qui permettent aux clients de masquer les numÃ©ros de cartes de crÃ©dit dans le serveur pour prÃ©venir les fuites de donnÃ©es sensibles

â¢ Une authentification des utilisateurs via les serveurs Radius

â¢ Des sauvegardes FTP automatiques et planifiÃ©es

â¢ Un nouvel outil dâimport/export pour les politiques de sÃ©curitÃ© spÃ©cifiques et la possibilitÃ© de cloner automatiquement ces politiques

â*Les applications Web sont des bases essentielles au fonctionnement des entreprises aujourdâhui. Câest pourquoi les organisations mettent maintenant lâaccent sur la protection des donnÃ©es dâapplications web ultra sensibles et rÃ©glementÃ©es,*â dÃ©clare **Michael Xie**, fondateur, Directeur Technique et Vice-PrÃ©sident du service technique chez Fortinet. â*La compromission de donnÃ©es dâapplications Web peut avoir des consÃ©quences dÃ©vastatrices. Vol dâidentitÃ©, espionnage industriel, fraude financiÃ¨re, impact nÃ©gatif sur la valeur de la marque et le retour de bÃ¢ton potentiel au niveau de la fidÃ©litÃ© du client en sont juste quelques exemples. Câest pourquoi nous apportons continuellement des mesures de sÃ©curitÃ© dâapplications web innovantes sur le marchÃ©. Cette derniÃ¨re version de notre firmware FortiWeb est un autre exemple de notre engagement pour sÃ©curiser les infrastructures dâapplications web de nos clients.*â

DisponibilitÃ©

La version du firmware FortiWeb 4.0 MR2 est dÃ©sormais disponible.