TOUTE L'ACTUALITÉ / SÉCURITÉ

Le code source des applications web reste très vulnérable

Maryse Gros, publié le 17 Février 2020

Entre 2018 et 2019, le nombre de vulnérabilités a baissé d'un tiers dans les applications web analysées par Positive Technologies. Celui-ci en a pourtant trouvé en moyenne 22 par entreprise les 38 applications scrutées. Une vulnérabilité sur 5 présente un degré de sévérité élevé.

Parmi les vulnérabilités des applications web répertoriées par l'OWASP, open web application security project, les mauvaises configurations de sécurité figurent parmi les plus couvertes, note le rapport de Positive Technologies. (Crédit Photo : Geralt/Pixabay)

Si la sécurité des applications web a continué de s'améliorer en 2019, avec un nombre moyen de vulnérabilités en recul d'un tiers et une baisse de 17% des applications contenant des failles à haut risque, certains domaines laissent toujours à désirer, pointe le rapport « Web Application Vulnerabilities and Threats : Statistics for 2019 » du spécialiste en sécurité Positive Technologies, installé à Moscou et Londres. Pour le réaliser, ses experts en sécurité ont analysé 38 applications web entièrement fonctionnelles. Celles-ci provenaient pour 26% du secteur financier, pour 21% des télécoms, pour 16% du secteur industriel, pour 29% d'entreprises IT et pour 8% de services administratifs.

Dans 9 cas sur 10, il était possible d'attaquer les visiteurs des sites web de différentes façons : redirection vers une ressource contrôlée par un pirate, vol d'identifiants par du phishing ou infection de l'ordinateur avec un malware. Des accès non autorisés aux applications pouvaient se faire sur 39% des sites et un contrôle complet du système intervenir sur 16% des applications web. Sur 8% des systèmes, ce contrôle permettait d'attaquer le réseau local. Enfin, ces analyses ont montré que la fuite de données sensibles constituait une menace dans 68% des applications web, la plupart d'entre elles étant de nature personnelle (47% des vols ou concernant des identifiants (31%).

Risque d'injection de scripts dans 53% des cas

82% des vulnérabilités se trouvaient dans le code d'application, indique le rapport. Mais comparé à 2018, le nombre moyen de vulnérabilités par application a baissé d'un tiers, à 22, dont 4 ayant une sévérité élevée. Une faille sur 5 présentant un degré sévérité élevée. Les vulnérabilités les plus couramment rencontrées sont liées dans 84% des cas à de mauvaises configurations de sécurité et dans 53% des cas à des risques d'injection de scripts (XSS) qui peuvent conduire à capturer les identifiants de session des utilisateurs. Suivent, dans 45% des cas, les problèmes liés à l'incapacité de restreindre correctement le nombre de tentatives d'authentification ce qui peut être exploité par des attaques de force brute pour accéder à l'application. Dans 37% des cas, les experts de Positive Technologies ont trouvé des problèmes de contrôle d'accès. La moitié des applications web testées constituaient de systèmes de production.

Malgré ces analyses peu rassurantes, Positive Technologies constate que les entreprises prennent plus sérieusement en considération la sécurité de leurs applications web, non seulement celles qui s'adressent au public mais aussi aux utilisateurs internes. Le spécialiste en sécurité rappelle deux principes de base : corriger toutes les failles détectées aussi rapidement que possible et automatiser les processus lorsque c'est possible. Elle recommande pour se faire de former les équipes aux méthodes de développement sécurisées et, notamment, d'installer des pare-feux pour application web.

Article rédigé par
Maryse Gros
Journaliste, chef de rubrique LMI

Une erreur dans l'article ?
Proposez nous une correction

Cet article vous a plu ? **Partagez le !**

A lire aussi

4 jours en moyenne pour pirater un réseau d'entreprise

Commentaire

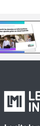
anakore (Membre) - 28/02/2020 à 09h40

Il faut sans cesse penser à tout même pour faire des choses simple il faut penser à "celui qui aurait envie d'utiliser la page ou l'application à d'autres fins que celle pour laquelle elle est faite" ce qui complique tout mais ne pas le faire c'est vraiment aller au devant des ennuies en créant un écosystème miné de partout qui tôt ou tard se retournera contre l'entreprise donc en faisant les choses bien dès le départ ça évite d'avoir à tout refaire de A à Z une fois qu'un problème de hacking tait son apparition ; car un code bien fait laisse peu d'entrée (peu de failles) alors qui si c'est fais à la va vite les canaux d'entrées sont si nombreux qu'il est pratiquement impossible de savoir par où la menace est arrivée forçant alors à tout refaire de A à Z et se traduisant par des dépenses phénoménales puisque pendant ce temps l'activités de l'entreprise peut être au point mort ...

SUR LE MÊME THÈME

Patch Tuesday avril 2024 : Microsoft comble 149 failles

FIC 2024 : LAnssi détaille son marathon cybersécurité



IBM et Fortinet déploient une appliance virtuelle pour protéger la sécurité du cloud

Avec YesWeHack, Louis Vuitton cherche des failles et sensibilise