https://www.brege.net/veilletechno/spip.php?article112

Planète Techno-collège

Je soutiens le Logiciel Libre
Je suis adhérent de l'April !

Par Jean-Luc GENET
Professeur de technologie

Firefox fait un sans faute lors d'un audit réalisé par l'agence allemande de sécurité informatique, qui le r nde comme étant le ur le plus sécurisé

Date de mise en ligne : lundi 21 octobre 2019

- VEILLE -

Firefox est le seul navigateur à avoir obtenu un sans-faute lors d'un récent audit réalisé par l'agence allemande de sécurité informatique - l'Office fédéral allemand de la sécurité de l'information (ou le Bundesamt für Sicherheit in der Informationstechnik - BSI). La BSI a testé Mozilla Firefox 68 (ESR), Google Chrome 76, Microsoft Internet Explorer 11 et Microsoft Edge 44. Les tests n'incluaient pas d'autres navigateurs tels que Safari, Brave, Opera ou Vivaldi.

L'audit a été effectué à l'aide de règles détaillées dans une directive pour les « navigateurs sécurisés modernes » publiée par le BSI le mois dernier, en septembre 2019.

La BSI utilise normalement ce guide pour conseiller les agences gouvernementales et les entreprises du secteur privé sur les navigateurs sécurisés. L'agence allemande de cybersécurité a publié une première directive relative aux navigateurs sécurisés en 2017, mais a revu et mis à jour les spécifications au cours de l'été.

La BSI a mis à jour son guide afin de prendre en compte les mesures de sécurité améliorées ajoutées aux navigateurs modernes, telles que HSTS, SRI, CSP 2.0, la gestion de la télémétrie et des mécanismes améliorés de gestion des certificats.Selon le nouveau guide de la BSI, pour être considéré comme « sécurisé », un navigateur moderne doit satisfaire à ces exigences minimales :

- doit prendre en charge TLS ;
- doit avoir une liste de certificats de confiance ;
- doit prendre en charge les certificats de validation étendue (EV) ;
- doit vérifier les certificats chargés par rapport à une liste de révocation de certification (CRL) ou à un protocole OCSP (Online Certificate Status Protocol) ;
- le navigateur doit utiliser des icônes ou des couleurs vives pour indiquer le moment où les communications avec un serveur distant sont chiffrées ou en texte clair ;
- les connexions aux sites Web distants exécutés avec des certificats arrivés à expiration ne doivent être

autorisées qu'après accord de l'utilisateur ;

- doit prendre en charge la sécurité du transport strict HTTP (HSTS) (RFC 6797) ;
- doit prendre en charge la politique de même origine (SOP) ;
- doit prendre en charge la politique de sécurité du contenu (CSP) 2.0 ;
- doit prendre en charge l'intégrité des sous-ressources (SRI) ;
- doit prendre en charge les mises à jour automatiques ;
- doit prendre en charge un mécanisme de mise à jour distinct pour les composants et extensions cruciaux du navigateur ;
- les mises à jour du navigateur doivent être signées et vérifiables ;
- le gestionnaire de mots de passe du navigateur doit stocker les mots de passe sous une forme chiffrée ;
- l'accès au coffre-fort de mots de passe intégré au navigateur ne doit être autorisé qu'après que l'utilisateur a entré un mot de passe principal ;

- l'utilisateur doit pouvoir supprimer les mots de passe du gestionnaire de mots de passe du navigateur ;
- les utilisateurs doivent pouvoir bloquer ou supprimer les fichiers témoins ;
- les utilisateurs doivent pouvoir bloquer ou supprimer l'historique de saisie semi-automatique ;
- les utilisateurs doivent pouvoir bloquer ou supprimer l'historique de navigation ;
- les administrateurs d'organisation doivent être en mesure de configurer ou d'empêcher les navigateurs d'envoyer des données de télémétrie / d'utilisation ;
- les navigateurs doivent prendre en charge un mécanisme permettant de rechercher des contenus / URL nuisibles ;
- les navigateurs devraient permettre aux organisations d'exécuter des listes noires d'URL stockées localement ;
- doit prendre en charge une section de paramètres dans laquelle les utilisateurs peuvent activer / désactiver les plug-ins, les extensions ou JavaScript ;
- les navigateurs doivent pouvoir importer des paramètres de configuration créés de manière centralisée, idéal pour les déploiements d'entreprise à grande échelle ;

- doit permettre aux administrateurs de désactiver les fonctionnalités de synchronisation de profil dans le cloud ;
- doit être exécuté après son initialisation avec des droits minimaux sur le système d'exploitation ;
- doit prendre en charge le sandboxing. Tous les composants du navigateur doivent être isolés les uns des autres et du système d'exploitation. La communication entre les composants isolés ne peut s'effectuer que via des interfaces définies. L'accès direct aux ressources de composants isolés ne doit pas être possible ;
- les pages Web doivent être isolées les unes des autres, idéalement sous la forme de processus autonomes. L'isolation au niveau des threads est également autorisée ;
- les navigateurs doivent être codés à l'aide de langages de programmation prenant en charge les protections de mémoire de pile et de tas ;
- le fournisseur de navigateur doit fournir des mises à jour de sécurité au plus tard 21 jours après la publication d'une faille de sécurité. Si le fournisseur de navigateur principal ne fournit pas de mise à jour de sécurité, les entreprises doivent passer à un nouveau navigateur ;
- les navigateurs doivent utiliser des protections de la mémoire du système d'exploitation telles que la randomisation du format d'espace d'adresse ou la prévention de l'exécution des données (DEP) ;
- les administrateurs d'organisation doivent être en mesure de réglementer ou de bloquer l'installation de modules complémentaires / extensions non autorisés.

Voir la suite en ligne...