Le célèbre gestionnaire de mots de passe LastPass hacké

	Le célèbre gestionnaire de mots de passe LastPass hacké

Deux chercheurs ont décortiqué le service en ligne et ont réussi à déchiffrer la base de mots de passe par le biais du processus de récupération de compte.

Diffusé aussi bien auprès du grand public que des entreprises, LastPass est certainement l'un des gestionnaires de mots de passe les plus populaires du moment. Mais est-il réellement sécurisé?
Les hackers Alberto Garcia et Martin Vigo – tous les deux membres de l'équipe sécurité de l'éditeur saleforce.com – ont décortiqué ce service par rétro-ingénierie et viennent de présenter le résultat de leur recherche à l'occasion de la conférence Black Hat Europe 2015. Ils ont trouvé une série de failles qui permettent, dans certains cas précis, d'accéder au Saint Graal : la base de mots de passe.
Dans un premier scénario, ils supposent que l'attaquant a réussi à s'implanter sur l'ordinateur de la personne ciblée, après un première infection. L'une des vulnérabilités présentées par les deux chercheurs – et qui a depuis été patchée – est d'utiliser le processus de récupération de compte. C'est une fonctionnalité fort utile pour les utilisateurs qui ont la mémoire qui flanche, mais qui s'appuie sur un élément fort bizarre: un mot de passe OTP (One Time Password) qui est généré par défaut et stocké en clair sur la machine. En l'intégrant dans une fausse requête de récupération par une requête HTTP, les deux hackers arrivent à ouvrir une session LastPass et à récupérer la version chiffrée de la base de mots de passe.

Un mot de passe boosté aux stéroïdes
Mais ce n'est pas tout: ils reçoivent aussi une version chiffrée de la clé qui permet de déchiffrer la base. Mais le sésame pour déchiffrer cette clé n'est pas très loin: c'est un dérivé de l'OTP par hachage (SHA-256). Bingo, la base est ouverte. Et le mieux dans cette affaire, c'est que cette procédure de récupération court-circuite les protections additionnelles que l'utilisateur peut mettre en place, telles que l'authentification à double facteur ou la restriction d'accès en fonction de l'adresse IP. « D'une certaine manière, l'OTP est un master password boosté aux stéroides », souligne les deux chercheurs, qui ont rapporté leur trouvaille à LastPass.
L'éditeur a, depuis, déployé un correctif qui empêche la création de fausses requêtes de récupération. Par ailleurs, il a introduit il y a quelques semaines un deuxième facteur d'authentification pour valider cette procédure, au travers d'un code envoyé par SMS. Il est vivement recommandé d'activer cette option baptisée « SMS Recovery » dans les paramètres du compte. Les hackers ont également rappelé dans leur présentation qu'il ne fallait jamais cocher la case « Mémoriser le mot de passe » dans le plugin Lastpass. En septembre 2014, ils avaient en effet montré qu'il était possible de le récupérer assez facilement, une fois que l'on a accès à la machine.
Attaque par JavascriptL'autre scénario imaginé par MM. Garcia et Vigo est celui d'un attaquant qui a réussi à accéder aux serveurs de LastPass. Théoriquement, une telle attaque ne devrait pas permettre d'accéder aux mots de passe d'un utilisateur car ils sont stockés de manière chiffrée. Mais les deux chercheurs ont trouvé un moyen détourné. Le service en ligne utilise du code Javascript pour pouvoir renseigner automatiquement les champs d'authentification dans une page web – ce qui est bien pratique.
Exécuté localement sur la machine de l'utilisateur, ce code peut accéder aux identifiants d'un compte en ligne. En insérant son propre code Javascript dans les serveurs de LastPass, un attaquant pourrait alors facilement récupérer ces données secrètes. On peut donc se demander si un tel service est réellement une solution face à des organisations telles que la NSA qui pourraient contraindre l'éditeur à intégrer leur propre code sur leurs serveurs…
Pour autant, pas la peine de jeter le bébé avec l'eau du bain. « LastPass s'est montré très réactif face à ces failles et les a réparé pour la plupart en l'espace de 72 heures », soulignent les chercheurs qui, par ailleurs, continuent à utiliser ce service. Car en dépit des failles potentielles que peut avoir un gestionnaire de mots de passe, ce sera toujours mieux que de noter ses mots de passe dans un tableur !

Source : http://www.01net.com/actualites/black-hat-2015-ils-ont-hacke-lastpass-le-celebre-gestionnaire-de-mots-de-passe-929666.html
Par Gilbert KALLENBORN

Kaspersky dévoile les limites de la maison connectée

	Kaspersky dévoile les limites de la maison connectée

Le spécialiste de la sécurité informatique Kaspersky vient de publier une étude mettant en lumière les failles de sécurité de plusieurs objets connectés pour la maison.

La société démontre comment le fameux Google Chromecast permet aux hackers de prendre contrôle de toute une maison 'connectée'.
Le rapport fait froid dans le dos…
Les rapports sur le manque de sécurité de certains objets connectés fleurissent sur internet, à l'instar de celui particulièrement alarmant publié par HP il y a quelques mois.
Malheureusement, ces problèmes de sécurité ne sont pas issus de la science-fiction, mais peuvent être à terme de vraies menaces pour les utilisateurs.
Kaspersky s'est intéressé aux objets connectés pour la maison, et en a choisi aléatoirement quatre différent qu'il a analysé :
la célèbre clé HDMI Google Chromecast, une caméra par IP connectée en Wi-Fi, une machine à café connectée ainsi qu'un hub de surveillance pour la maison. Il démontre ensuite pas-à-pas comment le Chromecast permet à un hacker de contrôler tous les autres appareils connectés dans la maison.
Forcer l'utilisateur à dévoiler le mot de passe du Wi-FiSans pour autant rentrer dans les détails techniques (disponibles dans le rapport), voici comment procède un hacker pour prendre contrôle de la maison :
• il utilise tout d'abord la vulnérabilité du Google Chromecast découverte en 2014 avec l'aide d'un Rickmote Controller. Cela lui permet ainsi de corrompre le contenu affiché sur la télévision et afficher un message d'erreur obligeant le propriétaire à changer le mot de passe du Wi-Fi, ou redémarrer le routeur.
• Une faille similaire a été découverte dans la machine à café connectée, qui n'a pas été nommée car la faille n'est toujours pas résolue.
• Une fois que le hacker possède le mot de passe du Wi-Fi de la maison, il peut ensuite facilement se connecter à la caméra de surveillance, et contrôler les allers et venues des personnes de la maison. Un cambrioleur peut ensuite s'introduire tranquillement dans la maison en utilisant un aimant suffisamment puissant et un vêtement capable de cacher la chaleur humaine. Pourquoi une telle tenue vestimentaire ? Les détecteurs de mouvements et de chaleur du hub de sécurité testé par Kaspersky pouvaient être facilement corrompus avec les méthodes assez simples d'utilisation.
Piratage : Une grand-mère se fait insulter par sa Smart TV ! Dans son communiqué, Kaspersky livre quelques conseils aux utilisateurs de tels produits pour se protéger un maximum, et éviter une attaque de grande ampleur.
A l'heure actuelle, réaliser un tel piratage reste cependant hautement complexe, et il est fortement probable que les cambrioleurs se contenteront encore pendant quelques temps de solutions plus classiques…

Ci-dessous, l'infographie qui résume la démarche de Kaspersky :

Lire la suite…

Comme tout professionnel de l'informatique et de l'Internet, il est de mon devoir de vous informer que vous devez mettre en conformité et déclarer à la CNIL tous vos traitement de données à caractère personnel (factures, contacts, emails…).
Même si remplir un formulaire de déclaration à la CNIL est gratuit, il vous engage cependant, par la signature que vous apposez, à respecter point par point la loi Informatique et Libertés. Cette démarche doit commencer par une analyse précise et confidentielle de l'ensemble de vos systèmes de traitements de données. Nous pouvons vous accompagner pour vous mettre en conformité avec la CNIL, former ou accompagner un C.I.L. (correspondant CNIL) ou sensibiliser les agents et salariés à l'hygiène informatique.
Besoin d'informations complémentaires ?
Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !
Source : http://www.stuffi.fr/piratage-kaspersky-devoile-les-limites-de-la-maison-connectee/

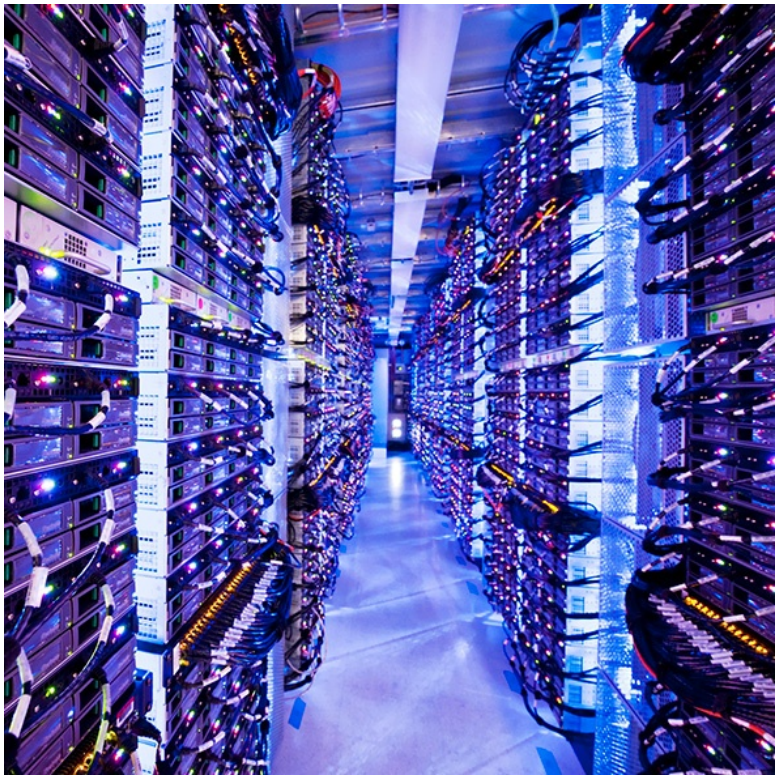
Microsoft stockera les données de ses clients européens en Allemagne

Microsoft stockera les données de ses clients européens en Allemagne

Le groupe américain Microsoft a annoncé mercredi que les données « cloud » de ses clients européens seraient dorénavant stockées dans deux centres informatiques en Allemagne.

Filiale de Deutsche Telekom, T-Systems contrôlera et supervisera tous les accès aux données des clients. Les services fonctionneront sur un réseau privé entre les entreprises et les deux data centers loin de la jungle d'internet, ce qui évitera tout rapatriement d'infos.

Un changement de relations avec les hébergeurs européens?
Concurrent de Microsoft, Amazon dispose certes déjà de centres de stockage en Allemagne, précise le journal Die Zeit. Les sites existants Irlandais et Hollandais qui appartiennent à Microsoft vont il être aussi gérés d'une manière différente par des sous traitants locaux pour offrir des services plus sécurisés?



Comme tout professionnel de l'informatique et de l'Internet, il est de mon devoir de vous informer que vous devez mettre en conformité et déclarer à la CNIL tous vos traitement de données à caractère personnel (factures, contacts, emails…).
Même si remplir un formulaire de déclaration à la CNIL est gratuit, il vous engage cependant, par la signature que vous apposez, à respecter point par point la loi Informatique et Libertés. Cette démarche doit commencer par une analyse précise et confidentielle de l'ensemble de vos systèmes de traitements de données. Nous pouvons vous accompagner pour vous mettre en conformité avec la CNIL, former ou accompagner un C.I.L. (correspondant CNIL) ou sensibiliser les agents et salariés à l'hygiène informatique.
Besoin d'informations complémentaires ?
Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !
Source : http://www.canaltogo.com/2015/11/14/localisation-des-donn-es-dans-le-cloud-quand-microsoft.html

Amazon Selling $40 Android Tablets That Come With Pre-Installed Malware

Amazon Selling $40 Android Tablets That Come With Pre-Installed Malware

Amazon is selling tablets from third-party manufacturers on its website that are preloaded with malware allowing hackers to take control of those devices remotely.

The malware-ridden tablets have been purchased by over 17,000 people to date, according to researchers at Cheetah Mobile Security Lab. The tablets, which are not part of Amazon's own range of devices, come from budget Chinese tablet manufacturers eager to lure those looking for a bargain by offering the devices for as little as $40.

The researchers found the malware – a Trojan horse called Cloudsota – preinstalled on certain Android tablets, enables remote control of the infected devices and conducts malicious activities without user consent. The researchers said they are confident the hackers behind the Cloudsota malware are in China, as the tablets are manufactured there and much of the code is written in Chinese. Amazon has yet to respond to a request for comment from International Business Times about these tablets.

There are many negative reviews of the tablets on the website that make mention of the malware being preinstalled, and yet many of the infected tablets remain on sale.

Lire la suite…

Source :

http://www.ibtimes.com/amazon-selling-40-android-tablets-come-pre-installed-malware-2181424

Un outil gratuit pour immuniser les ordinateurs et bloquer les menaces du

ransomware CryptoWall 4.0

Un outil gratuit pour immuniser les ordinateurs et bloquer les menaces du ransomware CryptoWall 4.0

Les chercheurs spécialistes en malwares et experts en cyber-sécurité de Bitdefender ont développé un outil gratuit afin de stopper la propagation du malware CryptoWall 4.0. Ce logiciel permet aux utilisateurs d'immuniser leurs ordinateurs et de bloquer les tentatives de chiffrement de fichiers.

L'outil peut être installé et utilisé en tant que mesure préventive, comme un vaccin, exclusivement contre cette variante spécifique de ransomware. Si l'ordinateur est déjà infecté par CryptoWall 4.0, ce vaccin n'aidera pas à désinfecter la machine.

Les pays ciblés jusqu'ici, identifiés par Bitdefender, incluent : la France, l'Italie, l'Allemagne, l'Inde, la Roumanie, l'Espagne, les États-Unis, la Chine, le Kenya, l'Afrique du Sud, le Koweït et les Philippines.

Les serveurs de spam de CryptoWall 4.0 sont situés en Russie et le malware écrit en Javascript, télécharge le composant de ce ransomware depuis un serveur russe. Les investigations de Bitdefender révèlent aussi que l'algorithme de chiffrement utilisé est de l'AES 256. Seule la clef est chiffrée en RSA 2048, qui est un algorithme impossible à déchiffrer du fait de sa complexité, mais qui demande beaucoup de ressources. Les utilisateurs russes semblent être à l'abri.

Le malware ne poursuit pas le chiffrement s'il détecte que la langue du clavier est le russe.

Dans la lignée de ses prédécesseurs, CryptoWall est rapidement devenu un succès financier pour ses créateurs. De récents chiffres montrent que les dommages liés à CryptoWall 3.0 s'élèvent à 325 millions de dollars, uniquement aux États-Unis. Ce succès a incité d'autres groupes de cybercriminels à écrire un nouveau code qui utilise des algorithmes de chiffrage plus sophistiqués. Par conséquent, il devient de plus en plus difficile pour les éditeurs d'antivirus de déchiffrer le code et de proposer une solution.

Bitdefender rappelle aux utilisateurs que cet outil agit comme une couche supplémentaire de protection, qui intervient en complément d'une solution antimalware.

Les utilisateurs des solutions de sécurité Bitdefender 2016 sont d'ores et déjà protégés contre le chiffrement de CryptoWall. La nouvelle technologie anti-ransomware de Bitdefender, unique sur le marché, empêche le chiffrement de fichiers et documents personnels et protège ainsi contre tous les rançongiciels, même nouveaux et inconnus.

Téléchargez gratuitement ICI le vaccin de Bitdefender contre CryptoWall 4.0
http://labs.bitdefender.com/projects/cryptowall-vaccine-2/bitdefender-offers-cryptowall-vaccine/

Les chercheurs en malwares de Bitdefender ont analysé un échantillon de nouvelles souches du malware et ont observé de nettes différences entre CryptoWall 4.0 et ses prédécesseurs.

Source : http://www.globalsecuritymag.fr/Bitdefender-a-developpe-un-outil,20151110,57433.html

Le pire des ransomwares vous fait perdre vos données à vie

Le pire des ransomwares vous fait perdre vos données à vie

Recrudescence de l’hacktivisme et des extorsions en ligne en 2016 | Le Net Expert Informatique

Recrudescence de l’hacktivisme et des extorsions en ligne en 2016

Trend Micro publie son rapport annuel de prédictions de sécurité 2016 : “The Fine Line : 2016 Security Predictions”. L’an prochain, les extorsions, l’hacktivisme et les malware mobiles devraient continuer de se développer. En parallèle, les administrations et les entreprises adopteront une posture plus offensive en matière de cyber-sécurité.

« Nous pensons que 2016 sera une année majeure, tant pour les cybercriminels que pour ceux qui souhaitent s’en protéger », explique Raimund Genes, CTO de Trend Micro. « Les administrations, au même titre que les entreprises, prendront conscience des bénéfices qu’apporte l’anticipation dans le domaine de la cyber-sécurité, avec une évolution attendue du cadre réglementaire et une augmentation des recrutements de responsables cyber-sécurité au sein des organisations. Parallèlement, alors que les utilisateurs sont de plus informés sur les menaces en ligne, les cyber-pirates s’adapteront en concevant des schémas sophistiqués et personnalisés pour cibler les particuliers comme les entreprises. »

Selon ce rapport, 2016 marquera un tournant significatif dans le domaine de la publicité malveillante (malvertising). Rien qu’aux États-Unis cette année, 48 % des internautes utilisent déjà des logiciels permettant de bloquer les publicités. Alors que l’utilisation de ces logiciels a bondi de 41% en 2015 dans le monde, les annonceurs vont modifier leur approche de la publicité en ligne, tandis que les cybercriminels tenteront d’identifier de nouveaux moyens pour obtenir les informations personnelles des internautes.

L’extorsion en ligne devrait croître rapidement, en faisant la part belle à l’analyse psychologique des victimes et aux techniques d’ingénierie sociale. Les hacktivistes seront amenés à divulguer des informations toujours plus incriminantes, impactant fortement leurs cibles et encourageant les infections secondaires.

« Les hackers évoluent en permanence pour s’adapter à leur environnement et, alors que la publicité en ligne décline, nous assistons à une progression des ransomware », constate Tom Kellermann, Chief Cybersecurity Officer, Trend Micro. « Face à des investissements croissants en sécurité et une réglementation qui se durcit, ce sont précisément ces évolutions qui aboutiront à de nouveaux vecteurs et méthodes d’attaques toujours plus sophistiqués ».

Parmi les principales prédictions de Trend Micro pour 2016 :

Les cybercriminels devraient utiliser de nouvelles méthodes pour personnaliser leurs attaques, faisant certainement de 2016 une année historique en matière d’extorsion en ligne

Le nombre de malware mobiles devrait franchir la barre des 20 millions, affectant notamment la Chine, tandis que les nouveaux moyens de paiement en ligne deviendront les principales cibles à l’échelle mondiale

Les objets et équipements intelligents étant de plus en plus utilisés au quotidien par le grand public, au moins une faille de sécurité sur ces derniers devrait s’avérer mortelle

Les hacktivistes vont faire évoluer leurs méthodes d’attaque de façon à détruire systématiquement leurs cibles par des fuites de données de très haut niveau

Moins de 50% des organisations devraient disposer d’experts en cyber-sécurité au sein de leurs équipes d’ici à fin 2016

La croissance des solutions et services de blocage de publicités devrait inciter les cybercriminels à trouver de nouvelles méthodes pour cibler leurs victimes, entraînant ainsi un recul des publicités malveillantes

La réglementation va évoluer vers un modèle de cyber-sécurité mondiale, permettant des poursuites, des arrestations et des condamnations de cybercriminels plus efficaces

Pour en savoir davantage sur les prévisions de sécurité en 2016 de Trend Micro, rendez-vous sur : http://www.trendmicro.fr/renseignem…

Source : http://www.globalsecuritymag.fr/Predictions-2016-Trend-Micro,20151106,57314.html

Je Suis Paris | Le Net Expert Informatique

Je
Suis
Paris

Loin des spams, des arnaque et de tous les actes illicites que nous suivons sur Internet depuis plusieurs années, nous partageons notre peine avec les victimes des attentats de Paris de ce Vendredi 13 Novembre 2015.

Denis JACOPINI est Expert Informatique assermenté, consultant et formateur en sécurité informatique, en mise en conformité de vos déclarations à la CNIL et en cybercriminalité.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité, en accompagnement aux mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL et accompagnement de Correspondant Informatique et Libertés.
Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : Denis JACOPINI

Une grosse panne à l'aéroport d'Orly provoquée par un système tournant sous… Windows 3.1 | Le Net Expert Informatique

Une grosse panne à l'aéroport d'Orly provoquée par un système tournant sous… Windows 3.1

Le 7 novembre, soit samedi dernier, une énorme panne a cloué les avions au sol pendant plusieurs heures à l'aéroport d'Orly. Une panne provoquée par une panne informatique d'une des tours de contrôle qui scrute les données météo. Après plusieurs heures, le trafic a repris et l'histoire aurait pu s'arrêter là. Mais le Canard Enchaîné a révélé la vraie nature de cet incident.

L'hebdomadaire revient en effet sur cette panne. Selon lui, elle concernait le système Decor (qui fourni les données météo) tournant sous… Windows 3.1. Un OS sorti en 1992, tout de même. C'est à cause d'une défaillance de ce système que des milliers de passagers se sont retrouvés bloqués. Dans le Canard, un ingénieur de l'aéroport donne d'ailleurs son avis sur la situation :

Samedi matin, le trafic n'était pas vraiment dense. Mais imaginez, pendant la COP21, le ballet des chefs d'Etat perturbé à cause d'un logiciel informatique qui date de la préhistoire. De quoi aura-t-on l'air ?

C'est vrai que l'histoire est tout de même étonnante, voire pathétique. Mais comme l'affirme l'hebdomadaire, le ministre des transports prévoit de renouveler le parc informatique de l'aéroport à partir de 2017.

Source :
http://www.journaldugeek.com/2015/11/12/une-grosse-panne-a-laeroport-dorly-provoquee-par-un-systeme-tournant-sous-windows-3-1/

Une faille dans un composant expose des milliers d’applications Java | Le Net Expert Informatique

Une faille dans un composant expose des milliers d’applications Java

Découverte il y a 9 mois, une vulnérabilité non corrigée dans le composant Apache Commons Collections expose les serveurs d'applications Java à un sérieux risque d'exécution de code à distance.

La dernière faille critique Java en date a été découverte dans la bibliothèque Apache Commons qui regroupe un ensemble de composants Java dont la maintenance est assurée par l'Apache Software Foundation. La bibliothèque est utilisée par défaut dans plusieurs serveurs d'applications Java et dans des produits comme Oracle WebLogic, IBM WebSphere, JBoss, Jenkins et OpenNMS.

La vulnérabilité, précisément localisée dans le composant Collections d'Apache Commons, résulte directement de la désérialisation des objets Java. Dans les langages de programmation, la sérialisation désigne le processus de conversion des données en format binaire. Cette conversion permet le stockage des données dans un fichier ou dans la mémoire, ou leur envoi sur le réseau. La désérialisation est le processus inverse.

La vulnérabilité, signalée par les chercheurs Chris Frohoff et Gabriel Lawrence en janvier 2015 pendant une conférence sur la sécurité, n'a pas suscité beaucoup d'attention. Sans doute que la plupart des gens estiment que la responsabilité de la prévention des attaques exploitant le processus de désérialisation incombe aux développeurs d'applications Java et non aux créateurs de la bibliothèque.

« Je ne pense pas qu'il faut incriminer la bibliothèque, même si elle peut certainement être améliorée », a déclaré par courriel Carsten Eiram, responsable de la recherche dans l'entreprise de sécurité Risk Based Security.

« En définitive, une entrée non fiable ne devrait jamais être désérialisée aveuglément. Les développeurs devraient comprendre comment fonctionne une bibliothèque et valider chaque entrée au lieu de lui faire confiance ou espérer qu'elle effectue à leur place ce travail de sécurisation ».

Un correctif bientôt disponible

Vendredi dernier, la faille est revenue dans l'actualité : les chercheurs de l'entreprise de sécurité FoxGLove ont livré des exploits proof-of-concept pour WebLogic, WebSphere, JBoss, Jenkins et OpenNMS basés sur la vulnérabilité. Mardi, Oracle a publié un avis de sécurité comportant des instructions d'atténuation temporaires pour WebLogic Server en attendant le correctif permanent que l'éditeur est en train de mettre au point. Les développeurs d'Apache Commons Collections ont également commencé à travailler sur un correctif.

Apache Commons Collections contient une classe InvokerTransformer. La faille utilise la sérialisation Java et une méthode d'appel dynamique dite de réflexion sur la classe InvokerTransformer pour exécuter du code distant. Un attaquant pourrait fabriquer un objet sérialisé avec un contenu malveillant pour qu'il soit exécuté au moment de sa désérialisation par une application Java avec l'aide de la bibliothèque Apache Commons. « Prises séparément, la classe InvokerTransformer et la sérialisation ne sont pas en cause, mais dès qu'elles sont combinées, la question de sécurité apparaît », a déclaré Joshua Corman, CTO de Sonatype, une entreprise d'automatisation de la chaîne d'approvisionnement des logiciels qui aide les développeurs à suivre et à gérer les composants qu'ils utilisent dans leurs applications.

D'autres composants Apache Commons vulnérables

Joshua Corman et Bruce Mayhew, un autre chercheur en sécurité de Sonatype, pensent que le problème ne concerne pas uniquement le composant Collections d'Apache Commons. Selon eux, d'autres composants Java pourraient poser un problème identique. « Je peux vous assurer qu'aujourd'hui, un tas de gens passent les composants les plus courants au peigne fin pour identifier d'autres classes sérialisables qui pourraient permettre l'exécution de commandes à distance », a déclaré Bruce Mayhew. « Et parmi eux, il y a des gens bien intentionnés, mais probablement aussi des gens mal intentionnés ». Si l'on en croit les discussions en cours sur la recherche de bogues, InvokerTransformer n'est sans doute pas la seule classe vulnérable de l'environnement Apache Commons Collections. Trois autres classes pourraient présenter le même problème. Les chercheurs de FoxGLove Security se sont intéressés de près à des projets de logiciels publics utilisables en « commons-collection » hébergés sur GitHub et ils ont identifié 1300 sources possibles. Et il faut aussi prendre en compte les milliers d'applications Java qui utilisent la bibliothèque dans les environnements d'entreprise.

Même s'il y a une forte probabilité que le problème dépasse le composant Collections, les développeurs devraient essayer de retirer les commons-collections du classpath ou de supprimer la classe InvokerTransformer du fichier jar concerné tant qu'il n'y a pas de correctif disponible pour la vulnérabilité. Mais tous ces changements doivent être appliqués avec précaution, car ils peuvent rendre les applications inopérantes.

Source : http://www.lemondeinformatique.fr/actualites/lire-une-faille-dans-un-composant-expose-des-milliers-d-applications-java-62956.html

Par Lucian Constantin, IDG NS (adaptation Jean Elyan)