Adobe : failles critiques dans Acrobat et Reader | Le Net Expert Informatique

Adobe : failles critiques dans Acrobat et Reader

Ces vulnérabilités, qui ne seraient pas exploitées, feront l'objet d'un patch salvateur ce mardi, assure l'éditeur.

Nouvelle fournée de correctifs en prévision chez Adobe. L'éditeur prévient en effet ses utilisateurs qu'Acrobat et Reader sont victimes de failles critiques, permettant donc une prise de contrôle à distance. Un ou plusieurs patchs seront distribués ce mardi.
Adobe ne précise pas la teneur de ces vulnérabilités mais assure qu'elles ne sont pas exploitées. Adobe Acrobat XI et Reader XI (11.0.10 et versions précédentes), ainsi qu'Adobe Acrobat X et Reader X (10.1.13 et versions précédentes) pour Windows et OS X sont concernés.

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

Source : http://www.zdnet.fr/actualites/adobe-failles-critiques-dans-acrobat-et-reader-39819162.htm

Lenovo : l’outil de mise à jour était troué | Le Net Expert Informatique

	Lenovo : l’outil de mise à jour était troué

Trois mois après l'affaire Superfish, les PC du fabricant chinois Lenovo, premier acteur mondial sur ce segment, sont à nouveau dans la tourmente. Des chercheurs en cybersécurité de chez IOActive assurent que les utilisateurs d'ordinateurs de la marque seraient à nouveau exposés à un « risque de sécurité massif ».

Michael Milvich et Sofiane Talmat, les deux chercheurs, viennent de publier un avis de sécurité (http://www.ioactive.com/pdfs/Lenovo_System_Update_Multiple_Privilege_Escalations.pdf) où ils expliquent que le service de mises à jour « System Update » de Lenovo est complètement troué.
System Update assure la mise à jour de la couche logicielle maison présente sur les ordinateurs Lenovo. Un outil pratique, mais qui n'était pas fiable jusqu'à récemment.
Ce service, qui permet aux clients de télécharger les derniers pilotes et logiciels Lenovo, dont les correctifs de sécurité, est victime de vulnérabilités importantes, qui permettent des attaques par escalade de privilèges.
L'une d'entre elle permet de contourner les contrôles de validation et de remplacer les programmes Lenovo proposés au téléchargement par des logiciels malveillants, et directement exécutés sur la machine par System Update. Une autre faille assure au pirate la possibilité d'exécuter ses propres commandes sur l'ordinateur piraté.

Un patch disponible
Les vulnérabilités affectent Lenovo System Update 5.6.0.27 et les versions antérieures. Le fabricant chinois a publié un patch le mois dernier pour corriger les failles de sécurité. Il est donc indispensable pour les clients de la marque de télécharger la mise à jour de sécurité pour ne pas courir le risque de compromettre leurs machines (https://support.lenovo.com/us/en/product_security/lsu_privilege).
Ces vulnérabilités ont été découvertes en février dernier, en plein milieu de l'affaire Superfish. Pas mesquin, IOActive a contacté Lenovo pour lui faire part de ses découvertes et lui permettre de déployer des correctifs de sécurité. Reste que la réputation de Lenovo commence à pâtir de ces multiples affaires de failles béantes.

Source : http://www.zdnet.fr/actualites/lenovo-l-outil-de-mise-a-jour-etait-troue-39819028.htm
Par Guillaume Serries

Alerte : La campagne d’un annonceur de Google détournée par des pirates | Le Net Expert Informatique

Alerte : La campagne d’un annonceur de Google détournée par des pirates

Des chercheurs en sécurité de la société néerlandaise Fox-IT ont repéré une campagne malveillante quand les annonces diffusées par Engage Lab, un partenaire de Google en Bulgarie, ont commencé à rediriger les utilisateurs vers le Nuclear Exploit Kit. Les kits d'exploit sont des plates-formes d'attaques basées sur le web dont l'objectif est d'exploiter les vulnérabilités des navigateurs et de leurs plug-ins pour infecter les ordinateurs des utilisateurs avec des malwares.

LNuclear Exploit Kit cible spécifiquement les vulnérabilités dans Flash Player d'Adobe, Java d'Oracle et Silverlight de Microsoft. « On dirait que l'ensemble du domaine engagelab.com, sa publicité et sa zone d'ID, est actuellement redirigé vers un domaine qui, à son tour, redirige vers le Nuclear Exploit Kit, attestant d'un éventuel piratage de ce revendeur de services de publicité partenaire de Google », a déclaré le chercheur de Fox-IT, Maarten van Dantzig dans un blog.
Ces redirections ont été stoppées tard dans la journée, ce qui montre que Google ou Engage Lab ont pris certaines mesures. Mais aucun n'a répondu aux demandes de commentaire de nos confrères d'IDG News Service. On ne sait pas combien de sites, ni combien d'utilisateurs ont été touchés, mais, selon Maarten van Dantzig, Fox-IT « a détecté une quantité relativement importante d'infections et de tentatives d'infection de nos clients par ce kit d'exploit ». Les chercheurs de Fox-IT n'ont pas encore identifié le malware distribué par cette campagne. Le problème du « malvertising », ces campagnes de fausses publicités qui détournent les internautes vers des pages web infectées, existe depuis plusieurs années et ne cesse de prendre de l'ampleur.
Et, même si les grands réseaux de publicités affirment avoir mis en place des défenses sophistiquées, les attaquants trouvent toujours de nouveaux moyens pour les contourner. Ces attaques sont particulièrement dangereuses, car elles n'ont pas besoin de rediriger les internautes vers des sites Web obscurs pour diffuser leur malware. Une fois que les attaquants parviennent à pousser leurs annonces malveillantes sur un grand réseau de publicité, celles-ci s'affichent sur des sites populaires dans lesquels les utilisateurs ont généralement confiance.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.lemondeinformatique.fr/actualites/lire-la-campagne-d-un-annonceur-de-google-detournee-par-des-pirates-60793.html
Par Jean Elyan

Europol a démantelé un réseau de pirates contrôlant des millions d'ordinateurs | Le Net Expert Informatique

Europol a démantelé un réseau de pirates contrôlant des millions d'ordinateurs