La foudre frappe des serveurs Google rendant des données momentatnément inaccessibles | Le Net Expert Informatique

	La foudre frappe des serveurs Google rendant des données momentatnément inaccessibles

A la suite d'un orage en Belgique, des serveurs appartenant à Google ont été privés de courant avec pour conséquence l'inaccessibilité de certaines données personnelles.

La foudre peut frapper deux fois au même endroit, la preuve un bâtiment situé en Belgique a reçu jeudi dernier quatre éclairs en l'espace d'un orage. Celui-ci, un data-center abrite des centaines de serveurs appartenant à Google. A l'intérieur de ceux-ci étaient stockées les données personnelles de nombreux utilisateurs et lorsque la foudre a frappé, le courant a sauté.
La BBC relate que cet aléa météorologique a eu quelques conséquences pour certains utilisateurs du service de stockage en ligne Google Drive. Leurs données ont en effet été momentanément inaccessibles.
Contacté par MyTf1news, le géant de l'Internet a réagi. « C'est une quantité infinitésimal qui a été affectée » a expliqué un responsable avant de poursuivre : « Aucune donnée n'a été perdue grâce à un système de sauvegarde décentralisé ». Dans les faits, il existait une copie des données affectées par la coupure de courant dans un autre data-center ailleurs sur la planète. Les documents des utilisateurs ont donc étaient inaccessibles juste le temps que ce système prenne le relai.
Les bâtiments de ce type sont généralement très bien protégés contre la foudre mais la répétition de ce phénomène n'avait apparemment pas été anticipée. Interrogé par la BBC, Justin Gale, un responsable d'Orion, une entreprise britannique spécialisée dans la protection des infrastructures contre la foudre revient sur le phénomène. L'éclair n'a pas besoin de frapper la structure en elle-même explique-t-il avant de préciser : « Un câble à un kilomètre peut être touché et le choc peut remonter jusqu'au data-center et tout faire disjoncter » détaille-t-il.
Dans un communiqué publié en ligne, Google relativise l'incident. Selon l'entreprise « moins de 0,000001% » de la surface des disques durs alloués à la zone géographique est concernée. La compagnie a néanmoins fait savoir qu'elle avait l'intention de renforcer ses protections contre les coupures de courant pour assurer la sécurité des données stockées sous sa responsabilité.

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

Source : http://lci.tf1.fr/high-tech/des-serveurs-de-google-frappes-par-la-foudre-des-donnees-personnelles-8646545.html
Illustration. Un éclair / Crédits : Comstock/Thinkstock

Écoutes : la mise en place de la PNIJ avance doucement | Le

Net Expert Informatique

Écoutes : la mise en place de la PNIJ avance doucement

Interpelé par un député qui se plaignait de la lenteur des procédures de réquisition effectuées auprès des opérateurs de téléphonie mobile, le ministre de l'Intérieur vient de donner quelques nouvelles de la Plateforme nationale des interceptions judiciaires (PNIJ), qui n'en finit pas d'accumuler du retard.

Initialement prévue pour fin 2013, la PNIJ n'est toujours pas opérationnelle. Cet énorme centre, placé dans les locaux du géant Thales, était pourtant censé faciliter le travail des enquêteurs – même si ce n'est pas l'avis de ses détracteurs. Autorisée par un décret publié en octobre au Journal officiel, cette plateforme doit en effet permettre de centraliser les nombreuses interceptions de correspondances ordonnées par la justice, de même que les réquisitions de données de connexion (quel abonné derrière telle adresse IP ou numéro de téléphone, etc).
Aujourd'hui, pour identifier un client d'Orange ou SFR, les réquisitions « sont transmises par les moyens de communication classiques – principalement le fax – et traitées par les employés des services des obligations légales des différentes sociétés », reconnaît ainsi le ministre de l'Intérieur au travers d'une réponse à une question écrite du député Jean-Luc Bleunven. Si le Code de procédure pénale permet théoriquement aux opérateurs de répondre à ces réquisitions par voie électronique, le locataire de la Place Beauvau explique qu'en pratique, ce n'est pas encore totalement le cas, en raison des retards de la PNIJ.

Une expérimentation menée depuis février en vue des identifications d'abonnés
Bernard Cazeneuve indique toutefois que des « protocoles » permettant de « mettre en place un système de réponse automatisé aux demandes de l'autorité judiciaire » a été signé « récemment » avec les quatre principaux opérateurs de téléphonie : Orange, SFR, Bouygues et Free. « L'expérimentation de la PNIJ sur ce point est en cours depuis le 9 février 2015 dans certains services d'enquête » poursuit le ministre de l'Intérieur. Selon lui, « les résultats sont extrêmement probants : les réponses aux réquisitions dont les opérateurs ont automatisé le traitement sont obtenues par les services d'enquête en quelques minutes contre plusieurs jours ou semaines auparavant ».
Restera maintenant à voir quand cette expérimentation limitée à quelques « services d'enquête » sera généralisée… Point sur lequel ne s'avance pas le premier flic de France.

Source : http://www.nextinpact.com/news/96181-ecoutes-mise-en-place-pnij-avance-doucement.htm
Par Xavier Berne

Un hack permet de pirater le bouton de commande physique d’Amazon | Le Net Expert Informatique

Un hack permet de pirater le bouton de commande physique d’Amazon

Le développement des objets connectés va constamment soulever davantage des questions de sécurité à mesure qu’ils se propageront. Un utilisateur américain en fait l’expérience en piratant une balise permettant de commander sur Amazon.

L’Amazon Dash se présente comme une balise adhésive. Disposée à l’endroit de son choix et reliée en WiFi, elle permet à une personne de passer une commande en appuyant sur un unique bouton physique. Aux Etats-Unis, le principe est simple puisqu’il autorise par exemple un foyer à se réapprovisionner en couche ou en lessive, lorsque ces produits viennent à manquer.
Le client n’a en effet que ce bouton à appuyer pour générer une nouvelle commande. Le procédé lui évite de se rendre en magasin ou même de commander en ligne par le biais des traditionnels sites de vente. Depuis plusieurs mois, ces boutons connectés sont donc déployés sur le territoire.
Surfer sur la vague des objets connectés n’est toutefois pas sans risques. Aux Etats-Unis, un spécialiste en sécurité est parvenu à intercepter le signal émis par ces boutons de commandes afin de commander autre chose que les objets normalement prévus. Dans une note, Ted Benson détaille sa démarche.
Il a ainsi rédigé un code en Python capable de sniffer les connexions WiFi et en particulier détecter ces boutons, lorsqu’ils émettent un signal. En les reprogrammant, il est en mesure de leur attribuer une autre tâche que la simple commande de produits. S’il ne s’agit que d’une expérience, le spécialiste demande à présent à l’ensemble des internautes de reproduire la démarche afin de trouver de nouveaux usages à ces boutons.

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu’intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d’entreprise.
Contactez-nous

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

Source : http://pro.clubic.com/it-business/securite-et-donnees/actualite-776644-dash-amazon-hack.html?estat_svc=s%3D223023201608%26crmID%3D639453874_1114740199#pid=22889469

Quatre jours de coupure informatique à la suite d’une

Cyberattaque | Le Net Expert Informatique

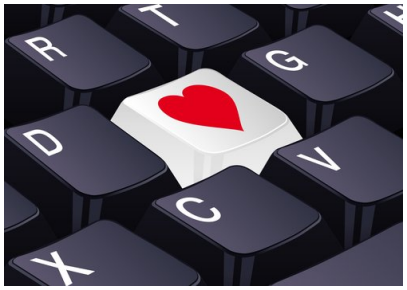
Le Parlement allemand va éteindre son système informatique pour quatre jours

Le Bundestag allemand plongera jeudi son système informatique dans un sommeil de quatre jours pour des opérations de maintenance, à la suite d'une vaste attaque informatique dont avait été victime fin mai la chambre basse du Parlement, a annoncé mercredi son président.

Passé ce délai, le système sera « à nouveau pleinement utilisable », soit à partir de lundi, a annoncé Norbert Lammert, le président du Bundestag.
Cette opération, initialement prévue quelques jours plus tôt, a dû être repoussée en raison du rappel des députés allemands pour voter mercredi sur le troisième plan d'aide à la Grèce.
La chambre basse du Parlement allemand avait été visée fin mai par une attaque informatique, qui s'était avérée beaucoup plus importante et vaste que prévue, les services du Bundestag peinant à la contrôler. Un ordinateur de la chancelière Angela Merkel avait également été touché.
Les hackers auraient pendant plusieurs semaines profondément infiltré le réseau informatique, parvenant à pirater des données, avait rapporté la presse allemande.
Les sites officiels de Mme Merkel, de la chancellerie et du Bundestag avaient déjà fait l'objet en janvier d'une cyberattaque, revendiquée par des hackers russes.
Selon des médias allemands, la dernière attaque contre le Bundestag viendrait aussi de Russie et pourrait avoir été lancée par des services de renseignements de ce pays.

Source : http://www.notretemps.com/internet/le-parlement-allemand-va-eteindre-son,i92309

Les données des utilisateurs du site de rencontres adultères AshleyMadison publiées | Le Net Expert Informatique



Les données des utilisateurs du site de rencontres adultères AshleyMadison publiées

Après avoir piraté les services du site AshleyMadison.com, les pirates mettent leurs menaces à exécution. Ils publient 9,7 Go de données concernant les utilisateurs du portail spécialisé dans les rencontres en ligne de personnes déjà en couple.

L'équipe de pirates ayant revendiqué l'attaque du site AshleyMadison.com en juillet dernier passe à l'offensive. Elle publie les données qu'elle détient, à savoir pas moins de 9,7 Go de données concernant 32 millions de comptes. Selon l'Impact Team, du nom des auteurs présumés de l'attaque, il s'agit là de l'ensemble de la base de données du site rencontres extraconjugales.
Les informations disponibles comprennent des historiques de paiements, des adresses postales et électroniques, le numéro de téléphone ou bien encore le nom des utilisateurs. La base de données ne comprend cependant pas les numéros de carte de paiement ou de crédit utilisés par les internautes, ni les mots de passe des visiteurs.
Plus précisément, les documents mis en ligne présentent ce que recherchaient les utilisateurs. Des mentions telles que « je recherche quelqu'un qui n'est pas heureux et qui souhaite un peu de plaisir » ou bien d'autres éléments censés générer des rencontres figurent dans cette publication.

Pour les pirates, AshleyMadison ment à ses clients
Lors du piratage en juillet dernier, les équipes ayant revendiqué l'attaque ont motivé leur action en qualifiant l'éditeur du site de menteur. Ils estiment qu'Avid Life Media (ALM) trompe ses utilisateurs lorsqu'il leur propose, par le biais d'une option payante, de supprimer la totalité de leurs informations personnelles sur le site.
Pour l'Impact Team, ces données resteraient bel et bien disponibles. C'est pourquoi ils publient cette base de données dont certains éléments datent de 2007. Ils mettent ainsi à mal la confidentialité des utilisateurs du service ainsi que les prétentions de la société éditrice.

Les revendications étaient également d'ordre moral puisqu'ils demandaient la fermeture d'un second site, Established Men. Les pirates jugeaient que le portail permettait de mettre en avant la « prostitution et le trafic d'êtres humains ».

Avid Life Media, le propriétaire du site, contre-attaque
De son côté, Avid Life Media présente à nouveau ses excuses face à cette fuite importante d'informations personnelles. La société précise auprès d'Ars Technica qu'elle ne confirme pas l'authenticité des documents mis en ligne et se retranche derrière les travaux en cours des autorités canadiennes.

Le professionnel rappelle cependant qu'il ne compte pas en rester là et note que : « cet événement n'est pas un cas d'hacktivisme mais un acte criminel. Il s'agit d'une action illégale menée à l'encontre des membres du site ». La société se dit ainsi confiante dans le fait que les autorités identifieront et poursuivront les personnes ayant mené ces attaques.

Source : http://pro.clubic.com/it-business/securite-et-donnees/actualite-776740-ashley-madison-hackers.html
Par Olivier Robillart

Les protocoles Internet de plus en plus exploités par les DDoS | Le Net Expert Informatique

Les attaques DDoS (Distributed Denial of Service) ont continué de s'intensifier au cours du second trimestre 2015. C'est notamment ce qui ressort du « State of the Internet Security Report » que vient de livrer Akamai (disponible depuis cette page). Un rapport dédié à la sécurité désormais indépendant de l'analyse historique propre au trafic Internet et qui s'appuie notamment sur les données recueillies par Prolexis, spécialiste anti DDoS que le CDN a racheté en décembre 2013. Dans cette édition – la seconde sous cette forme -, Akamai a observé 352,55 millions d'attaques d'applications Web depuis son réseau.

Il en résulte que, entre début avril et fin juin 2015, pas moins de 12 attaques DDoS ont dépassé les 100 Gbit/s en intensité. La plus importante ayant atteint les 245 Gbit/s. Sur ces 12 épisodes, le taux d'envoi moyen de paquets IP par seconde s'est élevé à 46 millions (46 Mpps). Un record. 5 attaques dépassent les 50 Mpps et 1 atteint 214 Mpps. « Ce volume de paquets est capable d'emporter des routeurs de tiers 1 (chez les principaux opérateurs Internet de la planète, NDLR), comme ceux utilisés par les fournisseurs d'accès », signale Akamai pour souligner la puissance de ces agressions.

Le nombre d'attaques a doublé

Si les pics de bande passante sont en progression par rapport à ceux observés au cours des trois premiers mois de l'année, ils restent cependant, sur la période étudiée, inférieurs à ceux de 2014. Mais le nombre d'attaques DDoS à plus de 100 Gbit/s a doublé au second trimestre 2015 par rapport à la période équivalente de l'année dernière, et a progressé de 50% par rapport aux 8 attaques similaires du premier trimestre 2015.

Côté méthodologie, les attaquants se sont principalement servis des commandes SYN (demande de synchronisation) et SSDP (Simple Service Discovery Protocol) pour opérer leurs manœuvres, chacune comptant pour environ 16% du trafic DDoS du trimestre. « La prolifération des appareils résidentiels connectés à Internet et non sécurisés utilisant le protocole UPnP (Universal Plug and Play) continue à les rendre attractifs pour des utilisations de réflexion SSDP, commente Akamai. Pratiquement absentes il y a un an, les attaques SSDP ont figuré parmi les principaux vecteurs d'attaque de ces trois derniers trimestres. » Les débordements SYN et UDP (transmission de manière simplifiée entre deux machines) restent, pour leurs parts, parmi les vecteurs les plus communs à toutes les attaques volumétriques. Mais ce trimestre voit également arriver l'exploitation des flux ACK (propre à la confirmation de la réception des données).

La faille Shellshock vecteur d'attaques

Si, comme par le passé, la moitié des attaques DDoS du deuxième trimestre exploitent plusieurs méthodes d'attaque simultanées, une stratégie masquant souvent des services en ligne dédiés à ce genre d'opérations malveillante selon Akamai, une partie de l'autre moitié s'en distingue en s'appuyant sur des bots (ordinateurs contrôlés par les pirates) similaires à Spike et IptabLes/IptabLex, le réseau de machines Linux infectées récemment exploité pour lancer des attaques DDoS.

L'exploitation de la faille Shellshock, un bug de l'interpréteur de commande Bash révélé en septembre 2014, figure en bonne place dans les vecteurs d'attaques aux côtés de XSS (cross-site scripting), SQLi (injection SQL) et LFI (local file inclusion) notamment. Shellshock se retrouve en effet dans 49% des attaques d'applications Web. Et compte pour 95% de toutes les attaques en HTTPS. « Néanmoins, modère Akamai, 95% des attaques Shellshock ont visé un unique client de l'industrie des services financiers, dans une campagne persistante qui s'est déroulée sur les premières semaines du trimestre. » Le nom de l'entreprise en question reste évidemment confidentiel. Mais la part des attaques HTTPS face à HTTP passe de 9% au premier trimestre à 56% au deuxième. Shellshock, SQLi et LFI combinent à eux trois 93% de l'ensemble des attaques.

WordPress, un vivier de bot

Selon Akamai, la plate-forme WordPress constitue un vivier de réseaux bot pour les pirates. Un phénomène qui s'explique par le manque de sécurisation des plugins de l'outil d'édition de sites web. Sur 1 322 greffons et thèmes publics étudiés par le CDN, 25 affichaient une ou plusieurs vulnérabilités totalisant 49 exploitations potentielles pour dresser des armées de PC zombies. Quant on sait que WordPress motorise environ 25% de l'ensemble des sites Web de la Toile, ça laisse songeur.

Akamai s'est également penché sur le cas de Tor, le réseau de routeurs décentralisés qui accorde un certain niveau d'anonymat à ceux qui l'utilisent. Il s'avère que, si 99% des attaques constatées ne sont pas lancées depuis Tor, 1 requête sur 380 provenant du réseau anonyme est d'origine malveillante. Contre 1 pour 11 500 requêtes pour les adresses IP non-Tor. « Pour autant, bloquer le trafic Tor pourrait avoir des conséquences négatives sur les affaires, commente Akamai. […] Si le réseau Tor représente un risque élevé pour les sites en matière de sécurité, il fournit également un bénéfice économique potentiel à certaines industries. » Le commerce en ligne, en premier lieu.

Source : http://www.silicon.fr/protocoles-internet-toujours-plus-exploites-attaques-ddos-124403.html
Par Christophe Lagane

Attention aux fausses mises à jour de Windows 10 dissimulant des Ransomware ! | Le Net Expert Informatique

Attention aux fausses mises à jour de Windows 10 dissimulant des Ransomware !

Il n'a pas fallu longtemps pour voir apparaitre les premières tentatives d'escroquerie autour de la mise à jour vers Windows 10 proposée par Microsoft depuis le 29 juillet 2015. Une première campagne de Ransomware vient d'être détectée.

Cette campagne s'appuie sur l'actualité brulante du moment, à savoir le lancement de la version finale de Windows 10 par Microsoft. L'objectif est de tromper les utilisateurs au sujet du téléchargement de la mise à jour gratuite. Il télécharge en réalité des fichiers malveillants sur leurs ordinateurs.

Définition d'un Ransomware selon Wikipédia:
Un Ransomware ou rançongiciel, est un logiciel malveillant qui prend en otage des données personnelles. Pour ce faire, un rançongiciel chiffre des données personnelles puis demande à leur propriétaire d'envoyer de l'argent en échange de la clé qui permettra de les déchiffrer.

Windows 10, un contexte idéal pour les Ransomware
Disponible depuis quatre jours seulement, Windows 10 est désormais installé sur des dizaines de millions d'ordinateurs et Microsoft entrevoit une accélération de la demande. Windows 10 est l'actualité du moment et surtout un contexte idéal pour des campagnes de Ransomware. L'équipe Cisco Talos vient d'en détecter une.
Ses créateurs utilisent une adresse IP attribuée à la Thaïlande. Ils sont à l'origine d'un envoi massif d'emails soigneusement construits afin d'inviter leurs destinataires à installer Windows 10.
Ces e-mails s'accompagnent d'une pièce jointe, une archive ZIP, qui contient un exécutable qui lance CTB-Locker. Si l'antivirus présent sur la machine ne le détecte pas ou si l'archive en question n'a pas été vérifiée par un système web comme VirusTotal, le résultat est peu glorieux avec un verrouillage de données et l'apparition d'un message.
Celui-ci demande de payer une somme afin de rendre de nouveau accessible les données de l'ordinateur. Voici le message en question.

L'équipe Cisco explique qu'il s'agit ici d'une méthode
« standard […], en utilisant un cryptage asymétrique qui permet aux adversaires de crypter les fichiers de l'utilisateur sans avoir la clé de déchiffrement présente sur le système infecté. »
Les utilisateurs ont seulement quatre jours pour payer la «rançon». Les pirates se cachent au travers de « Tor » et de la monnaie « Bitcoin » afin d'être anonymes. Ils profitent ainsi de leur campagne de logiciel malveillant avec un risque minimal. L'équipe Cisco Talos recommande de créer des sauvegardes régulières de son PC et de stocker les archives en dehors de tous services en ligne.

Source : http://www.appy-geek.com/Web/ArticleWeb.aspx?regionid=2&articleid=45798024&source=hootsuite
Par GINJFO

Les publicités piégées au ransomware se multiplient | Le Net Expert Informatique

ransomwa

Les publicités piégées au ransomware se multiplient

Une nouvelle campagne d'infection via des annonces publicitaires falsifiées sévit sur plusieurs sites populaires comme Weather.com ou Drudgereport.com, prévient KnowBe4.

Une nouvelle campagne de « malvertizing » sévit sur Internet. Weather.com, Drudgereport.com, wunderground.com, des sites qui génèrent plusieurs millions de visites mensuelles, en seraient victimes. L'infection serait en train de s'étendre à Ebay.com et AOL.com, indique Stu Sjouwerman, le CEO de KnowBe4, une société spécialisée dans le conseil en sécurité qu'il a créée avec Kevin Mitnick, l'un des hackers les plus médiatiques des années 90. Rappelons que ce dernier avait accédé aux systèmes de grandes entreprises américaines, ce qui lui a valu 5 ans d'emprisonnement en 1995.
Selon KnowBe4 la campagne infectieuse diffuserait des ransomware de type CryptoWall. Une fois installée dans le système, généralement des PC sous Windows, cette bestiole crypte les fichiers locaux. Pour pouvoir les déchiffrer et y accéder de nouveau, ses auteurs réclament une rançon de 500 dollars (montant généralement constaté aujourd'hui), généralement en Bitcoin, à la victime. Un récent rapport de Proopoint estimait que les attaques par CryptoWall généraient jusqu'à 25 000 dollars par jour de revenus pour les pirates. Selon des chercheurs de Dell SecureWorks, plus de 830 000 personnes dans le monde avaient été victimes d'un ransomware fin 2014.

Adspirit.de, le propagateur
Ce ne pas les sites eux-mêmes qui sont infectés, mais la plate-forme de diffusion des annonces publicitaires qui, indirectement, contribue à la propagation infectieuse en distribuant les fichiers publicitaires malveillants. Dans le cas présent, le réseau Adspirit.de serait à l'origine de la contamination. L'entreprise sert en effet d'intermédiaire entre les annonceurs et les sites « afficheurs ». Quand les annonceurs sont des pirates, les choses se compliquent. Les publicités infectieuses ne se distinguant pas en apparence des réclames légitimes, il est facile de tomber dans le panneau. Un simple clic sur ces pubs déclenche le processus d'infection.
Pire : dans de nombreux cas, leur simple affichage suffit à enclencher le mécanisme de contamination par exploitation d'une faille système (particulièrement celle du player Flash, ou encore de Java, d'où l'importance d'appliquer régulièrement ses mises à jour de sécurité) sans aucune intervention de l'utilisateur. Pour s'en prémunir, KnowBe4 préconise d'utiliser le mode « clic-to-play » qui impose une intervention manuelle pour dérouler un contenu publicitaire en Flash, voire de supprimer le plugin d'Adobe de son navigateur. Ou encore d'installer un bloqueur de publicités comme Ad-Blocker, utilisé par 200 millions de personnes dans le monde et honni par la presse en ligne qui l'accuse d'un manque à gagner de 45 millions de dollars rien qu'aux Etats-Unis.
Si KnowBe4 nomme bien Adspirit.de comme étant la source de cette campagne infectieuse dans son communiqué, le nom du diffuseur n'apparaît pas dans le billet de blog de la société de conseils en sécurité. Aucune alerte n'a cependant été émise du côté du réseau allemand. Quelques semaines auparavant, c'est Yahoo qui avait exposé ses visiteurs à une campagne d'attaques par publicités déguisées.

Source : http://www.silicon.fr/nouvelle-vague-publicites-piegees-ransomware-124341.html
Par Christophe Lagane

Alerte à partager : Urgent – Mise à jour URGENTE votre Windows | Le Net Expert Informatique

Alerte à partager : Mise à jour URGENTE votre Windows

La découverte d'une faille critique ou Zero-Day dans Internet Explorer a contraint Microsoft à anticiper le prochain Patch Tuesday pour délivrer un correctif de sécurité. Le navigateur Edge de Windows 10 n'est pas affecté.

Selon le bulletin d'alerte de l'éditeur, une vulnérabilité expose les internautes, lors d'une visite sur un site piégé, à une exécution distante de code sur les postes Windows affectés. La faille zero-day (CVE-2015-2502) repose sur la façon dont Internet Explorer gère les objets dans la mémoire.
Une exploitation réussie de la vulnérabilité permet à l'attaquant d'obtenir les mêmes droits que l'utilisateur actif sur la session Windows, précise le bulletin de sécurité. Par conséquent, les utilisateurs dont le compte est paramétré avec les droits administrateurs sont les plus exposés.

Windows 10 et Edge : « la meilleure protection »
Selon Microsoft, aucun signe ne laisse penser que cette faille logicielle soit déjà exploitée pour des attaques. Un correctif est donc disponible, à télécharger sur le site de l'éditeur ou via Windows Update.
A noter que le navigateur Edge, le logiciel par défaut sur Windows 10, n'est pas affecté par la faille de sécurité. « Nous recommandons à nos clients d'utiliser Windows 10 et le navigateur Microsoft Edge pour la meilleure protection » ne manque d'ailleurs pas d'ajouter l'éditeur.
La découverte de cette vulnérabilité critique d'Internet Explorer est attribuée à un ingénieur de Google, Clement Lecigne. C'est le deuxième mois consécutif que Microsoft doit diffuser un correctif en-dehors de son cycle habituel.

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

Source : http://www.zdnet.fr/actualites/microsoft-corrige-en-urgence-toutes-les-versions-windows-39823686.htm

---

Cyber-attaque de pompe à morphine : mise en garde de

la FDA | Le Net Expert Informatique

Cyber-attaque de pompe à morphine : mise en garde de la FDA

La FDA met en garde contre les risques de prise de contrôle à distance des pompes à morphine ou PCA (de type PCA analgésie autocontrôlée par le patient) de type Symbiq Infusion System (produites par la marque Hospira). Ces pompes sont généralement prescrites dans le cadre de soins de suite ou d'hospitalisations à domicile.

Elles sont reliées sans fil aux systèmes de communication de l'hôpital pour transmettre des données sur les doses utilisées quotidiennement. Ces informations sont utilisées par les médecins pour adapter les protocoles de soins.

Un cyber-spécialiste démontre la possibilité d'attaques

C'est la deuxième fois en 4 mois que les pompes de ce fabricant font l'objet de cyber attaques, les premiers modèles impliqués étaient les LifeCare PCA3 et PCA 5 qui permettent de délivrer différents types de médicaments ou de traitements intraveineux.

Hospira a annoncé avoir cessé de produire les pompes en question ainsi que les Symbiq Infusion Systemet la FDA met en garde les établissements et les professionnels en les incitant à ne plus utiliser ces dispositifs.

Le département de la sécurité américain s'est saisi du dossier en raison des risques associé à ces cyber attaques (surdoses, ou sous dosage).

C'est un cyber spécialiste – Billy Rios [2] – qui a le premier soulevé cette question sur son blog et expliquant qu'il avait pu modifier les paramètres des pompes à distance sans disposer des codes spécifiques à chaque machines qui sont théoriquement indispensables pour modifier les doses.

Aucun cas de cyber attaque n'a été rapporté en utilisation thérapeutique aux Etats-Unis jusqu'à présent.

Une utilisation contrôlée en France – en théorie

En France, les pompes de type PCA sont utilisées dans les hôpitaux, en hospitalisation à domicile (dans un contexte de lien ville-hôpital), dans les services de soins palliatifs et dans certains centres de soins de suites/maisons de retraite médicalisés.

Elles servent à la prise en charges des douleurs chroniques de l'adulte, essentiellement d'origine cancéreuses et en soins palliatifs. Les principales marques de pompes à morphine de type PCA sont marque Vygon, Baxter, Gelstar, CADD Legacy et Rytmic Plus.

Les pompes à PCA électroniques ne doivent – en théorie – être manipulées que par le personnel médical (médecin ou IDE). Chaque marque diffuse avec le matériel un manuel d'utilisation pour les soignants et des codes permettant de modifier les paramètres ou changer les piles. Mais depuis quelques années, on peut trouver sur Internet des copies de ces manuels, ce qui pourrait permettre aux utilisateurs qui auraient récupéré les codes de façon illicite de modifier les paramètres dans un but de mésusage.

Source : http://www.medscape.fr/voirarticle/3601689
Par Dr Isabelle Catala avec Robert Lowes