Faille de sécurité chez Lenovo

	Faille de sécurité chez Lenovo

Sur certains modèles Lenovo, le lecteur d'empreinte ouvre une faille de sécurité potentielle. (CCM) – C'est une faille de sécurité importante que vient de révéler Lenovo. Le système de reconnaissance d'empreintes digitales de certains modèles de la marque laisse un accès aux mots de passe et aux identifiants de connexion.

Cette faille sur le lecteur d'empreinte du clavier a été découverte par un chercheur en sécurité de l'entreprise Security Compass. Le problème concerne plusieurs modèles d'**ordinateurs PC Lenovo**, comme les portables ThinkPad, ThinkCentre et ThinkStation qui tournent sous Windows 7, 8 et 8.1. Après une année 2015 compliquée pour la marque, Lenovo connaît de nouveaux problèmes de sécurité. Tout vient du **Lenovo Fingerprint Manager Pro**. Ce logiciel permet l'identification d'empreintes, à la manière de ce que fait le TouchID de l'iPhone. Il sert à l'identification des utilisateurs du PC, et il peut aussi être utilisé pour des identifications sur différents sites web…[lire la suite]

Les utilisateurs sont donc invités à installer la **version 8.01.87 de Fingerprint Manager Pro** pour résoudre ce problème.

Réagissez à cet article

Source : *Faille de sécurité chez Lenovo*

Failles dans les microprocesseurs Meltdown & Spectre

Failles dans les microprocesseurs Meltdown & Spectre

Ces derniers jours, il y a eu beaucoup de bruit dans la sphère de la sécurité informatique. Les mots Meltdown et Spectre ont fait la une de plusieurs journaux et sites d'information, qu'ils soient spécialisés ou généralistes. Cet article est une mise à plat de ma compréhension du sujet, une explication qui j'espère permettra à d'autres de mieux comprendre les mécanismes et la portée de ces attaques.

Les mécanismes en jeu

Ces deux attaques sont différentes de celles dont nous entendons parler majoritairement. Elles touchent le matériel, ou *hardware*, et non pas des applications. Pour comprendre ces attaques, il est nécessaire de faire un petit récapitulatif sur le fonctionnement et l'optimisation d'un processeur.

Fonctionnement d'un processeur

Un processeur, ce n'est rien d'autre qu'une calculatrice. Au début, des calculs étaient envoyés à un processeur, celui-ci effectuait les calculs qu'on lui envoyait dans l'ordre, les uns après les autres, puis il retournait les résultats.

Lorsqu'un programme est exécuté, les données à traiter sont dans la mémoire vive (qu'on appelle aussi simplement *mémoire*), ou RAM. Pour traiter une instruction, les données nécessaires au traitement doivent être envoyées depuis la mémoire vive vers la mémoire interne du processeur pour qu'il les traite. Ensuite, le résultat est enregistré à nouveau en mémoire.

Si le temps de traitement des données par le processeur est environ le même que le temps de récupération des données en mémoire, tout ça se coordonne très bien. En effet, pendant que le processeur traite une instruction, les données de la prochaîne instruction sont rapatriées, permettant d'avoir un flux tendu.

Avec le temps, le matériel a évolué, et les processeurs sont devenus très, très rapides. Tellement rapides qu'ils ont largement devancé les accès en mémoire. Ainsi, aujourd'hui, le traitement d'une instruction se fait environ en 0.5 nano-seconde, tandis qu'un accès mémoire se fait en 20 nano-secondes.

Par conséquent, si jamais le processeur traitait les instructions linéairement, il passerait la plupart de son temps à attendre les données, au lieu de travailler.

C'est pourquoi les constructeurs se sont penchés sur le sujet afin d'optimiser le processus de traitement de leurs processeurs…[lire la suite]

Réagissez à cet article

Source : *Attaques Meltdown & Spectre – hackndo*

Alerte : Deux failles importantes découvertes. Mettez à jour !

	Alerte : Deux failles importantes découvertes. Mettez à jour !

De quoi s'agit-il ? Le 3 janvier 2018, deux failles importantes de sécurité baptisées Meltdown et Spectre ont été révélées publiquement. Ces failles touchent à des niveaux variables les microprocesseurs de la très grande majorité des ordinateurs personnels (PC), mais aussi des serveurs informatiques, des tablettes, des téléphones mobiles (smartphones) dans le monde entier.

Quel est le risque ?

Un attaquant qui parviendrait à exploiter ces failles pourrait avoir accès aux informations personnelles des utilisateurs des machines vulnérables (données personnelles, mots de passe, coordonnées bancaires…).

Ces failles étaient connues depuis quelques mois maintenant des principaux constructeurs de microprocesseurs (Intel, AMD, ARM), des grands éditeurs de logiciels (Microsoft, Apple, Google, Mozilla…) ainsi que des éditeurs d'anti-virus qui préparaient depuis lors des correctifs de sécurité.

Suite aux révélations publiques de ces failles, la manœuvre s'accélère pour les corriger avant que les cybercriminels n'arrivent à en profiter et les premiers correctifs ont commencé à être diffusés.

Etes-vous concernés ?

Certainement. Comme évoqué ci-dessus, la grande majorité des ordinateurs, des tablettes, des téléphones mobile, mais aussi des serveurs dans le monde entier est touchée par ces failles. Ces failles concernent aussi bien les machines qui fonctionnent sous Microsoft Windows, que celles qui fonctionnent sous Apple macOS-iOS, Google Android ou les différentes versions de GNU/Linux.

Que devez-vous faire pour vous protéger ?

Vous assurer de bien installer toutes les mises à jour de sécurité que vous avez peut-être déjà reçues et que vous allez recevoir dans les prochains jours, semaines voire mois des éditeurs de vos systèmes d'exploitation (Microsoft, Apple, Google, GNU/Linux), de vos navigateurs Internet (Microsoft, Google, Mozilla, Apple…), de vos anti-virus.

Pensez à bien vérifier que tous les systèmes de vérification des mises à jour de vos équipements sont bien activés.

Pensez à contrôler également que les mises à jour de sécurité que vous réalisez proviennent bien de vos éditeurs et constructeurs. Des cybercriminels pourraient essayer de profiter de cet événement pour se faire passer pour vos éditeurs ou constructeurs et vous envoyer de fausses mises à jour qui contiendraient un virus. N'acceptez donc par exemple aucune mise à jour que vous recevriez par mail, car c'est une pratique totalement inhabituelle.

Si vous faites vos mises à jour, serez-vous complètement protégés ?

Ce n'est pas complètement certain. Rien ne permet même d'attester que ces failles pourront être intégralement corrigées. Mais les différents correctifs de sécurité qui seront diffusés rendront certainement la tâche bien plus difficile pour les cybercriminels qui voudraient en tirer partie.

Toutes ces mises à jour qui arrivent en même temps peuvent-ils produire des dysfonctionnements de vos matériels ?

Ce n'est pas impossible. Mais le risque de dysfonctionnement est certainement bien moindre que celui de se voir voler ses données personnelles les plus confidentielles (mots de passe, numéros de carte bancaire…) par des cybercriminels.

Vous avez entendu que vos matériels risquaient de ralentir après les mises à jour de sécurité, qu'en est-il ?

Ce n'est pas impossible non plus, mais il est bien trop tôt pour l'affirmer. Vous pouvez même ne pas constater la moindre différence. Quoiqu'il en soit, si tel était le cas, mieux vaut aller un peu moins vite en sécurité, que plus vite en prenant des risques inconsidérés.

Vous avez entendu que ces failles étaient difficilement exploitables, alors devez-vous vraiment en tenir compte ?

Oui, car la cybercriminalité ne cesse de progresser en compétence technique. La vague d'attaques par le rançongiciel (ransomware) Wannacry du printemps 2017 est là pour le rappeler. A peine quelques semaines après la révélation d'une vulnérabilité de haut niveau, les cybercriminels ont réussi à l'exploiter pour une attaque qui a frappé le monde entier.

En conclusion ?

Ces failles sont sérieuses et touchent tous les équipements informatiques ou presque. Il est donc primordial de se sentir concerné et d'appliquer avec sérieux toutes les mises à jour de sécurité officielles que vous recevez de vos constructeurs ou éditeurs

[Original sur cybermalveillance.gouv.fr]

Réagissez à cet article

Source : *Alerte sécurité — Failles Meltdown & Spectre — CYBERMALVEILLANCE.GOUV.FR*

Alerte : une faille de sécurité critique découverte dans Thunderbird

La fondation Mozilla invite ses utilisateurs à migrer au plus vite vers la nouvelle mise à jour de son fameux logiciel de messagerie Thunderbird. Outre quelques améliorations, celle-ci colmate plusieurs failles de sécurité, dont une jugée critique.

Mozilla a publié le 22 décembre dernier sur son site un rapport détaillant les différentes vulnérabilités découvertes dans la précédente version de Thunderbird 52.5.1. L'une d'entre elles, jugée critique par la fondation, est une vulnérabilité de débordement de tampon affectant uniquement les utilisateurs de Windows. « *Un débordement de tampon se produit lors du dessin et de la validation d'éléments lors de l'utilisation de Direct 3D 9 avec la bibliothèque graphique*« , a déclaré Mozilla dans son avis de sécurité. « *Cela est dû à une valeur incorrecte transmise dans la bibliothèque lors des vérifications et entraîne un plantage potentiellement exploitable* ». Deux autres failles de sécurité classées « élevées » ont été également corrigées, dont une qui affectait les capacités du lecteur RSS de Thunderbird. La seconde pourrait potentiellement permettre à un attaquant de découvrir des données utilisateurs telles que ses identifiants. La nouvelle mise à jour 52.5.2 comprenant les correctifs peut être téléchargée directement sur le site de Mozilla…[lire la suite]

Réagissez à cet article

Source : *Thunderbird : une faille de sécurité critique découverte*

Prédictions cybersécurité 2018

En 2018, les cybercriminels vont continuer à exploiter les faiblesses inhérentes à la nature humaine pour dérober des informations personnelles, avec des changements significatifs dans les techniques de cyberattaques. Découvrez les grandes lignes de ces tendances qui rythmeront l'année 2018 selon Proofpoint.

L'email restera le vecteur de cyberattaque le plus utilisé

Vol de cryptomonnaie : de nouvelles menaces aussi répandues que les chevaux de Troie

Le facteur humain, toujours au cœur des cyberattaques

La menace grandissante des bots sur les réseaux sociaux

[cliquez pour plus de détails]

Réagissez à cet article

Source : *Prédictions cybersécurité 2018 – Global Security Mag Online*

DarkNet : Découverte d’une base de données de 1,4 milliards d’identifiants et mots de passe en clair

DarkNet : Découverte d’une base de données de 1,4 milliards d’identifiants et mots de passe en clair

Open data chez les cybercriminels ! La découverte a été annoncée par la société spécialisée en sécurité informatique 4iQ. Il s'agit de la plus importante base de données pirate jamais découverte en ligne. Elle pèse 41 Go.

La découverte de 4iQ date du 5 décembre et la société indique qu'elle se trouve sur un espace du Dark Web, sans préciser l'endroit (on se doute bine pourquoi). La base de donnée en question contient exactement ***1 400 553 869 identifiants et mots de passe en clair***, et un moteur de recherche dédié permet d'y accéder et d'y naviguer. Du vrai open data chez les pirates !…

[…]

[…]

N'oubliez pas les règles de sécurité pour réduire les risques de piratage de vos comptes ne ligne : changez régulièrement vos mots de passe, utilisez un générateur de mot de passe sécurisé (ou activez la double authentification lorsque c'est possible) et stockez vos identifiants / mots de passe de manière sécurisée via un gestionnaire de mot de passe…[lire la suite]

Réagissez à cet article

Source : *DarkNet : Découverte d’une base de données de 1,4 milliards d’identifiants et mots de passe en clair | UnderNews*

RGPD : Vol de données : la nouvelle norme

RGPD : Vol de données : la nouvelle norme

A six mois de l'entrée en vigueur du nouveau règlement européen sur la protection des données personnelles (RGPD) le 25 mai 2018 prochain, Proofpoint, spécialiste de la cybersécurité, dévoile les résultats de son étude paneuropéenne (Royaume-Uni, France, Allemagne) analysant le niveau de préparation des entreprises.

Les cyberattaques sont malheureusement devenues monnaie courante pour les entreprises qui doivent désormais intégrer pleinement les risques associés à leurs stratégies de sécurité pour se protéger. A l'image du piratage d'Equifax exposant les données personnelles de plus de 145 millions de citoyens américains ou du ransomware Wannacry ayant affecté plus de 200,000 ordinateurs dans 150 pays, tout le monde est concerné.

La France, semble particulièrement affectée, avec 61% des entreprises françaises qui déclarent avoir subi un vol de données personnelles durant les deux années écoulées (54% au Royaume Uni et 56% en Allemagne) et 78% d'entre elles qui redoutent un vol de données dans les 12 mois à venir (54% au Royaume-Uni et 46% en Allemagne).

Niveau de préparation RGPD : un décalage évident entre perception et réalité

Si les décideurs IT français semblent mieux préparés que leurs voisins (51% des répondants français pensent que leur organisation est déjà en conformité avec la réglementation RGPD, contre 45% au Royaume-Uni et 35% en Allemagne), l'étude révèle que plus d'une entreprise française sur cinq (22%) ne sera toujours pas en conformité avec la réglementation lors de son entrée en vigueur en mai 2018 (23% au Royaume-Uni et 34% en Allemagne). Un résultat finalement peu surprenant, considérant que seules 5% des entreprises auraient effectivement mis en place toutes les stratégies de gestion de données nécessaires pour garantir cette mise en conformité.

Les décideurs IT semblent pourtant conscients des enjeux, puisque 66% des répondants confient que leur budget a augmenté en prévision de l'entrée en vigueur de RGPD. Plus de sept entreprises sur dix en Europe ont par ailleurs monté des équipes projet dédiées RGPD et plus d'une sur quatre a désigné un responsable de la protection des données. A l'épreuve des faits, et alors que les entreprises avaient deux ans pour se préparer (adoption de la réglementation en avril 2016), seuls 40% des répondants révèlent que leur organisation a rempli un formulaire de mise en conformité RGPD…[lire la suite]

Réagissez à cet article

Source : *RGPD : 1 entreprise française sur 5 ne sera pas en conformité ! | UnderNews*

Objets connectés: attention, on vous espionne…

	Objets connectés: attention, on vous espionne…

Montre connectée. Enceintes connectées. Casque connectée. Jouets connectés… Autant d'appareils qui ont besoin d'Internet pour fonctionner correctement. Sauf qu'ils sont susceptibles d'être des espions. La plupart sont, en effet, vulnérables aux menaces.

En France, l'Association européenne de défense des consommateurs a pris les devants pour demander que les poupées connectées soient retirées des étagères pour Noël. Ces poupées connectées, d'un fabricant réputé, répond aux enfants. Les conversations ont été enregistrées au préalable. Toutefois, cela n'est pas conforme aux règles de protection des données des mineurs. En effet, n'importe qui peut s'y connecter à travers le Bluetooth et ainsi intercepter des conversations

Selon un informaticien, les parents ne réalisent pas ce qu'ils achètent. *«Ils ignorent les dangers des poupées ou des jouets connectés. Ils vont en acheter sans réaliser qu'il y a des failles de sécurité»*, fait-il valoir.

Pas de vérifications

Le fait est que tous les objets qui ont des fonctions Bluetooth et sont équipés de micros sont de parfaits espions. Grâce à des logiciels espions, des pirates peuvent écouter les conversations. Wikileaks a rendu public des documents, en mars dernier, prouvant que la *National Security Agency*, aux États-Unis, peut effectuer des écoutes…[lire la suite]

Réagissez à cet article

Source : *Objets connectés: attention, on vous espionne… | lexpress.mu*

Alerte ! Un virus «indétectable» pour Windows voit le jour

Alerte ! Un virus «indétectable» pour Windows voit le jour

Une nouvelle méthode permettant d'esquiver tous les logiciels antivirus a été présentée par les employés de la société enSilo lors de la conférence sur la cybersécurité Black Hat Europe 2017. Ce virus, restant invisible, serait susceptible d'affecter le fonctionnement de toutes les versions de Windows.

Dans le cadre de la conférence sur la cybersécurité Black Hat Europe 2017, les spécialistes de la société enSilo ont décrit une nouvelle méthode permettant d'effectuer une cyberattaque tout en restant indétectable par les antivirus. D'après les programmeurs, ce schéma, baptisé Process Doppelgänging, fonctionne sur toutes les versions de Windows.
Ainsi, les experts ont établi qu'avec l'utilisation des transactions NTFS, il était possible d'apporter des modifications dans un fichier. Ensuite, Process Doppelgänging est capable de masquer le chargement de ce fichier modifié. Pendant tout ce temps-là, l'antivirus ignore que l'ordinateur est la cible d'une attaque puisque le code malveillant utilisé par Process Doppelgänging ne laisse pas de traces sur le disque…[lire la suite]

Réagissez à cet article

Source : *Attention, danger! Un virus «indétectable» pour Windows voit le jour – Sputnik France*

Jouets connectés : Dangers pour votre vie privée dit la CNIL

	Jouets connectés : Dangers pour votre vie privée dit la CNIL

La Présidente de la CNIL met en demeure la société GENESIS INDUSTRIES LIMITED de procéder à la sécurisation de jouets connectés à destination d'enfants : la poupée « My Friend Cayla » et le robot « I-QUE ».

Le robot « I-QUE » et la poupée « My Friend Cayla » sont des jouets dits « connectés ». Ils répondent aux questions posées par les enfants sur divers sujets tels que des calculs mathématiques ou encore la météo. Les jouets sont équipés d'un microphone et d'un haut-parleur et sont associés à une application mobile téléchargeable sur téléphone mobile ou sur tablette. La réponse est extraite d'Internet par l'application et donnée à l'enfant par l'intermédiaire des jouets.

Alertée, en décembre 2016, par une association de consommateurs sur le défaut de sécurité des deux jouets, la Présidente de la CNIL a décidé de réaliser des contrôles en ligne en janvier et novembre 2017. Elle a par ailleurs adressé un questionnaire en mars 2017 à la société située à Hong-Kong.

Ces vérifications ont permis de relever que la société collecte une multitude d'informations personnelles sur les enfants et leur entourage : les voix, le contenu des conversations échangées avec les jouets (qui peut révéler des données identifiantes comme une adresse, un nom…) mais également des informations renseignées dans un formulaire de l'application « My Friend Cayla App ».

Plusieurs manquements à loi Informatique et Libertés ont été constatés dont notamment :

1.

Le non-respect de la vie privée des personnes en raison d'un défaut de sécurité

Les contrôleurs de la CNIL ont constaté qu'une personne située à 9 mètres des jouets à l'extérieur d'un bâtiment, peut connecter (ou « appairer ») un téléphone mobile aux jouets grâce au standard de communication Bluetooth sans avoir à s'authentifier (par exemple, avec un code PIN ou un bouton sur le jouet).

La personne située à une telle distance est en mesure d'entendre et d'enregistrer les paroles échangées entre l'enfant et le jouet ou encore toute conversation se déroulant à proximité de celui-ci.

La délégation de la CNIL a également relevé qu'il était possible de communiquer avec l'enfant situé à proximité de l'objet par deux techniques :

• soit en diffusant via l'enceinte du jouet des sons ou des propos précédemment enregistrés grâce à la fonction dictaphone de certains téléphones ;

• soit en utilisant les jouets en tant que « kit main libre ». Il suffit alors d'appeler le téléphone connecté au jouet avec un autre téléphone pour parler avec l'enfant à proximité du jouet.

La Présidente a considéré que l'absence de sécurisation des jouets, permettant à toute personne possédant un dispositif équipé d'un système de communication Bluetooth de s'y connecter, à l'insu des enfants et des propriétaires des jouets et d'avoir accès aux discussions échangées dans un cercle familial ou amical, méconnait l'article 1er de la loi Informatique et Libertés selon lequel l'informatique *« ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques ».*

2.

Le défaut d'information des utilisateurs des jouets

Alors que des informations personnelles sont traitées par la société, les contrôleurs de la CNIL ont constaté que les utilisateurs des jouets ne sont pas informés des traitements de données mis en œuvre par la société…[lire la suite]

Réagissez à cet article

Source : *Jouets connectés : mise en demeure publique pour atteinte grave à la vie privée en raison d'un défaut de sécurité | CNIL*