PIRATAGE

Log4Shell, la faille informatique qui fait trembler le web

Une faille découverte il y a peu pourrait entraîner des conséquences dramatiques dans les semaines à venir, puisqu'elle concerne un morceau de code extrêmement répandu dans les applications.

THOMAS CASAVECCHIA

Parmi les entreprises exposées figurent Microsoft, IBM, certains services d'Amazon ou encore Tesla. © PHOTO NEWS.

On risque d'en subir les répercussions pendant des mois », assure Axel Legay, professeur en cybersécurité à l'UCLouvain. La découverte d'une faille de sécurité il y a quelques jours a fait trembler le web sur ses fondations. C'est Chen Zhaojun, un chercheur de la société de commerce en ligne Alibaba, qui a découvert la faille et a alerté le monde de la cybersécurité le 24 novembre dernier.

La faille, rendue publique le 10 décembre dernier, a été évaluée à un niveau de menace de 10/10 par le Common Vulnerabilities and Exposures. On ne fait pas plus haut sur l'échelle de Richter du risque informatique.

Et ce tremblement de terre a fait vaciller quelques géants. Ainsi, Microsoft, IBM, certains services d'Amazon ou Tesla ont été exposés. Par mesure de précaution, les gouvernements canadiens et québécois ont même fait fermer pas loin de 4.000 sites gouvernementaux.

Concrètement, la faille permet aux personnes mal intentionnées de pénétrer incognito dans les serveurs pour y exécuter du code malveillant. Elle touche un bout de code open source tellement pratique et en dehors de tout soupçon qu'il est présent dans une très large part des sites web. Le nom de la faille ? Log4Shell, du nom des lignes de code exposé : Log4J.

Log4J est une bibliothèque codée en Java utilisée par les applications web. « On peut voir cette bibliothèque comme un journal des évènements de l'application, explique Jean-Michel Dricot, professeur de cybersécurité à l'ULB. Cela permet de consigner que telle personne s'est connectée au service à telle heure et a exécuté telle application. C'est ce que l'on appelle un log des infos. Cette bibliothèque est si simple, si efficace et open source, qu'on la retrouve dans la plupart des applications en ligne ».

Un risque pour les particuliers ?

Le risque pour Monsieur et Madame Toulemonde est relativement limité. Mais il n'est pas nul. On peut imaginer de nouvelles vagues de virus ou de cryptolockers. « De manière générale, il est recommandé d'effectuer les mises à jour de sécurité de son système d'exploitation et de ses logiciels au fur à mesure qu'elles sont disponibles », explique Jean-Michel Dricot. Les joueurs de Minecraft ont par exemple été particulièrement exposés aux cryptolockers. Microsoft a publié des mises à jour afin de combler la faille dans les jours qui ont suivi les attaques. TH.CA

De nombreuses PME menacées

Cette bibliothèque est même un des piliers des sites modernes. Une omniprésence qui multiplie bien entendu les risques. « D'habitude, lorsque l'on découvre une faille aussi critique, elle est circonscrite dans une application ou au sein d'un service particulier. Ici, l'outil d'Apache (l'ONG derrière l'outil, NDLR) est si répandu que de très nombreuses entreprises risquent d'être compromises, déplore Axel Legay. Et il faudra sans doute pas mal de temps avant que tous les correctifs ne soient déployés ».

D'autant plus qu'il n'est pas rare qu'une entreprise utilise le code défaillant sans même le savoir, via des logiciels externes. « Les PME et plus petites entreprises font souvent appel à des prestataires extérieurs pour leur réseau. Etant donné l'omniprésence de Log4J, nombreux sont ces derniers à l'utiliser. Et il faut que chaque prestataire publie son correctif afin que l'utilisateur final, l'entreprise, soit en sécurité ».

Déjà, les premiers effets de Log4Shell se font sentir. « Une analyse de Checkpoint, une des sociétés leaders de cybersécurité, a déjà identifié plus de 2 millions de tentatives d'exploitation de la faille, relate Jean-Michel Dricot. Et il y a des rapports qui font déjà état de groupes malveillants qui ont implanté des malwares ou des cryptolockers en vue d'extorquer des entreprises ou destinés à utiliser de la puissance de calcul afin de miner des cryptomonnaies. On imagine aussi sans peine que les groupes de pirates puissent dérober des données et des documents sensibles. Ces failles sont rarement non exploitées ».

Mais même une fois les mises à jour effectuées, les boites touchées ne sont pas sorties d'affaire. Une fois la brèche d'une coque de bateau colmatée, il faut encore vider l'eau de la cale. « Il est encore trop tôt pour mesurer l'impact concret de cette faille. Néanmoins, il n'est pas rare qu'un groupe malveillant qui a réussi à pénétrer un système informatique se fasse oublier quelque temps, avant de passer à l'action », note Katrien Eggers, porte-parole du Centre pour la cybersécurité en Belgique (CCB).

Un scénario catastrophe constituerait donc en une avalanche de ransomware et autres compromissions dans les semaines et mois à venir. Une sorte de séisme qui débuterait par ses répliques. Pour les experts en sécurité informatique, les vacances de fin d'année seront à l'évidence mouvementées.

petite gazette

Crottes et faux billets

Une crotte de chien sous son pied, ce n'est jamais agréable. De nombreuses villes luttent pour que les propriétaires ramassent les déjections canines.

La ville marnaise de Châlons-en-Champagne a mené une expérience et l'a filmée dans une vidéo devenue virale depuis quelques jours. Sur celle-ci, on peut voir des personnes filmées à leur insu qui promènent leur animal et se baissent pour ramasser... un billet de dix euros. Sauf que celui-ci est faux et contient un message de sensibilisation. « Si vous êtes capable de vous baisser pour ramasser ce (faux) billet, alors vous l'êtes aussi pour ramasser les crottes de votre chien. »

Chaque année, 4.500 litres de déjections canines sont ramassées par les services de la ville. 20MINUTES.FR

Dixit

« Le racisme et la haine ne sont pas inscrits dans les péchés capitaux, ce sont pourtant les pires... »

JACQUES PRÉVERT

Panique au supermarché

Une araignée a semé la panique dans un supermarché de la banlieue nord de Stuttgart, rapporte l'agence de presse DPA. Alors qu'un employé déballait une caisse de bananes dans les rayons du magasin, la petite bête a bondi hors de la boîte et s'est échappée. Par peur d'avoir affaire à une araignée dangereuse, les responsables du magasin ont préféré appeler la police, un expert en araignées ainsi qu'un exterminateur et un employé d'un service de sauvetage d'animaux pour rattraper l'arachnide.

Durant une heure et demie, le supermarché a fermé ses portes, le temps que les équipes trouvent l'araignée. Finalement, elle a été découverte dans un coin du magasin et la petite bête s'est avérée être totalement inoffensive, car c'était une araignée crabe. Plus de peur que de mal ! SOIRMAG

Le joli et cher pull de Noël de Kate Middleton

Ce vendredi avait lieu la journée internationale du pull de Noël et Kate Middleton n'a pas dérogé à la tradition. L'épouse du prince William a posé dans un cardigan rouge en maille à col Claudine, signé Miu Miu. Des spécialistes ont relevé son prix exorbitant: 1.400 euros. RTL INFO

Une défaite...

Ce dimanche 19 décembre, José Mendes, joueur du Cannet-Rocheville, club de football amateur des Alpes-Maritime, a demandé sa compagne en mariage sur la pelouse du stade Vélodrome de l'Olympique de Marseille. Un événement ayant eu lieu quelques minutes après la défaite 4-1 de son club face aux professionnels marseillais en 32es de finale de la Coupe de France.

... et une victoire

Alors que les deux équipes s'apprêtaient à regagner les vestiaires, José Mendes a fait sa demande sur le terrain, accompagné par quelques coéquipiers lui faisant une haie d'honneur. Sa compagne sera sa future femme puisqu'elle a accepté cette demande.

Le futur époux n'a pas pris part à la rencontre face à l'OM. Il était suspendu pour ce match. OUEST-FRANCE

Le père Noël...

Au coeur de l'Amazonie brésilienne, pas de traîneau pour le père Noël : juché sur la proue d'un grand bateau à moteur, il salue les enfants qui l'attendent de pied ferme sur la rive. Son habit rouge et blanc tranche avec le vert émeraude de la plus grande forêt tropicale du monde et les eaux brunes du fleuve Solimoes. « Joyeux Noël ! », s'écrie-t-il avant d'accoster dans la localité de Parana da Terra Nova, à 24 km de Manaus, la plus grande métropole amazonienne. Dans le cadre d'une opération de l'association Amigos do Papai Noel (Amis du Père Noël), il va à la rencontre de communautés pauvres de « Ribeirinhos », familles vivant sur les rives du fleuve, à 24 km de Manaus.

... se déplace en bateau

Quand il met enfin pied à terre, après trois heures de navigation, ce père Noël pas comme les autres ouvre grand les bras pour accueillir les bambins qui accourent vers lui. « On ne peut pas changer le monde, mais on peut faire sourire des enfants à Noël », confie Jorge Alberto, 57 ans, emmitouflé dans son épais costume.

Pour apporter les cadeaux à ceux qui vivent dans les zones les plus isolées, il doit parfois affronter un vrai parcours du combattant. AFP

Le microspcope de Darwin...

Le 15 décembre dernier, la maison de vente aux enchères Christie's a vendu un nouvel objet rare : un microscope ayant appartenu à Charles Darwin. Fabriqué en 1825, l'instrument a été réalisé par un certain Charles Gould. Il s'agit d'un des six derniers microscopes connus liés au célèbre naturaliste, mais le premier vendu aux enchères. D'après la maison de vente, la date de fabrication correspond au moment où Darwin menait des recherches sur les rives du Firth of Forth, un fleuve écossais.

...vaut une fortune

Le scientifique aurait par la suite cédé le microscope à son fils Leonard en 1864. L'objet est ainsi resté en possession de sa famille pendant 150 ans, avant d'être préposé aux enchères. « C'est incroyablement excitant de regarder à travers et de voir le monde microscopique tel que Darwin le voyait dans les années 1820 et 1830 », a indiqué le directeur du département « Instruments scientifiques, globes & histoire naturelle » de chez Christie's.

L'instrument avait été estimé entre entre 295.000 et 412.000 euros. Il a finalement été adjugé à 705.459,38 euros. SOIRMAG