15 avril 2025 - EDITION N°20

LES ACTUS CYBER DE LA SEMAINE

SWIPE A DROITE POUR EN SAVOIR PLUS →

MICROSOFT PATCH UNE ZERO-DAY UTILISÉE DANS UNE SÉRIE DE RANSOMWARES

Du 8 avril 2025

Parmi les 126 vulnérabilités corrigées par Microsoft dans sa dernière mise à jour de sécurité, l'une d'elles concernait une faille zero-day dans le système CLFS (Common Log File System) de journalisation, qui a été exploitée pour une série d'attaques par ransomware.

Le groupe qui a exploité cette vulnérabilité, nommé par Microsoft « Storm-2460 » a lancé des attaques contre des cibles variées : des entreprises technologiques et immobilières aux Etats-Unis, le secteur financier vénézuélien, une compagnie de logiciels espagnole et le secteur de la grande distribution saoudien.

Le procédé utilisé par le groupe dans l'exploitation de cette vulnérabilité est l'élévation de privilèges : les hackers parviennent à obtenir des privilèges utilisateurs suffisamment élevés pour pouvoir installer des malwares sur le système, modifier les fichiers registres et les fichiers systèmes critiques. Les hackers de « Storm-2460 » ont utilisé ce processus pour déployer massivement leur ransomware.

Cela illustre la dangerosité pour les systèmes de ces menaces 0-day, des failles non-détectées.

Source : https://cyberscoop.com/microsoft-patch-tuesday-april-2025/

LA COMMUNAUTÉ OPEN SOURCE DE SOURCEFORGE ABUSÉE

Du 8 avril 2025

Des hackers ont abusé de SourceForge, une plateforme très populaire dans la communauté open source, qui héberge et distribue des logiciels. Elle assure également le contrôle de version, le suivi des bugs et propose des forums dédiés.

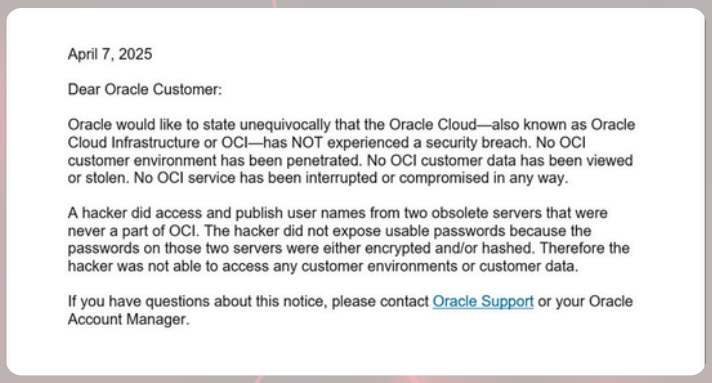
Ces acteurs se sont servis de la plateforme pour distribuer des faux add-ins Microsoft installant des malwares sur les systèmes des victimes et volant des cryptomonnaies.

Kapersky est à l'origine de la découverte de ces abus et a répéré 4 604 systèmes infectés situés pour la plupart en Russie.

Cela illustre l'ambivalence de l'open-source : les systèmes et logiciels basés sur l'open-source sont extrêmement manipulable gratuitement mais peuvent présenter des risques de sécurité plus élevés que les systèmes payants.

Source : https://www.bleepingcomputer.com/news/security/fake-microsoft-office-add-in-tools-push-malware-via-sourceforge/

ORACLE RECONNAÎT QUE DES « SERVEURS OBSOLÈTES » ONT ÉTÉ PIRATÉS MAIS NIE TOUTES FAILLES DANS SON CLOUD



April 7, 2025

Dear Oracle Customer:

Oracle would like to state unequivocally that the Oracle Cloud—also known as Oracle Cloud Infrastructure or OCI—has NOT experienced a security breach. No OCI customer environment has been penetrated. No OCI customer data has been viewed or stolen. No OCI service has been interrupted or compromised in any way.

A hacker did access and publish user names from two obsolete servers that were never a part of OCI. The hacker did not expose usable passwords because the passwords on those two servers were either encrypted and/or hashed. Therefore the hacker was not able to access any customer environments or customer data.

If you have questions about this notice, please contact Oracle Support or your Oracle Account Manager.

Du 9 avril 2025

L'entreprise américaine Oracle a été victime d'une cyberattaque en mars où 6 millions de données volées ont été mises en vente sur *BreachForums* par le hacker *rose87168* mais l'entreprise a nié systématiquement toute faille dans ses systèmes.

L'entreprise a finalement communiqué par mail à ses clients que les données volées proviennent de « deux serveurs obsolètes » mais insiste sur le fait que les serveurs « Oracle Cloud » n'ont pas été touchés n'impactant ainsi pas les données des clients et les services Cloud. Les données publiées ne seraient ainsi que des « noms d'utilisateurs issus de deux serveurs obsolètes qui n'ont jamais fait parti de l'Infrastructure Oracle Cloud » et donc que « le hacker n'a pas pu accéder aux environnements ou aux données des clients.

L'argumentaire principal de cet article démontre le jeu sur les mots d'Oracle : les vieux services Cloud d'Oracle (incluant ces deux serveurs obsolètes) ont été renommés « Oracle Classic » (touché par la cyberattaque) et permet donc à Oracle d'affirmer que les services « Oracle Cloud » n'ont pas été affectés.

Source : https://www.bleepingcomputer.com/news/security/oracle-says-obsolete-servers-hacked-denies-cloud-breach/

LES ATTAQUES PAR RANSOMWARE EN AUGMENTATION AU ROYAUME-UNI

Du 10 avril 2025

Les attaques par ransomwares (« rançongiciels ») sont en augmentation au Royaume-Uni mais le gouvernement note que les victimes ne reportent qu'assez peu auprès des autorités compétentes. Le gouvernement s'appuie sur les chiffres recueillis auprès de 2 180 entreprises, 1 081 associations caritatives et 574 institutions éducationnelles.

Comme en France, les institutions de santé et leurs affiliés sont visés : en novembre 2024, une attaque par rançongiciel a forcé un établissement du NHS (National Health Service, service de santé britannique) à annuler ses différents rendez-vous. Une autre attaque a mené à des pénuries de sang dans les hôpitaux britanniques.

Ces chiffres interviennent dans un contexte de changement politique au Royaume-Uni : le gouvernement réfléchit dans la prochaine U.K. Cyber Security and Resilience Bill à interdire aux entreprises du secteur public de payer des rançons et à les forcer à rapporter aux autorités compétentes tout incident cyber auxquelles elles feraient face dans les 72h.

Source : https://www.bankinfosecurity.com/ransomware-incidents-on-rise-in-uk-a-27971

LE DÉPARTEMENT DE L'INTÉRIEUR AMÉRICAIN LICENCIE DES EMPLOYÉS CLÉS DANS LA DÉFENSE CYBER AMÉRICAINE

Du 11 avril 2025

Le département de l'intérieur américain a licencié certains hauts responsables et vétérans de la branche cyber de l'institution, en charge de gérer les terres fédérales et les ressources naturelles du territoire américain sous administration fédérale (différent des ministères de l'intérieur en charge de la sécurité).

La raison officielle derrière ces licenciements est en apparence extrêmement politique : le DOGE (Department Of Government Efficiency)d'Elon Musk, dans sa quête vers la réduction de l'administration fédérale, cherche à réduire la masse salariale au sein des administrations fédérales. Cependant, certains officiels du gouvernement fédéral affirme qu'il s'agit en réalité d'une manœuvre pour permettre au DOGE d'accéder à des informations gouvernementales hautement sensibles et classifiées, allant jusqu'à accuser certains membres du DOGE de ne pas appliquer les protocoles de sécurité de ce type d'informations.

Il ne s'agit pas des premiers licenciements de l'administration Trump de personnels clés du monde de la cyber publique aux Etats-Unis, le directeur de la NSA et chef du U.S. Cyber Command ayant également été licencié.

Source : https://www.bankinfosecurity.com/interior-department-ousts-key-cyber-leaders-amid-doge-spat-a-27977

UN SERVICE DE LABORATOIRE AMÉRICAIN DÉCLARE UNE FUITE DE DONNÉES MASSIVES AVEC PLUS D'UN MILLION D'INDIVIDUS TOUCHÉS

Du 12 avril 2025

Laboratory Services Cooperative (LSC) est une organisation à but non lucratif qui fournit des services de laboratoire centralisés. Elle est relativement sensible car elle gère certains centres du Planned Parenthood (l'organisme à but non lucratif américain de planification familiale) aux Etats-Unis dans un contexte où beaucoup d'Etats américains sont de plus en plus restrictifs sur le droit à l'avortement. La fuite a exposé les données sensibles de 1,6 millions de personnes.

Une enquête interne a révélé que les activités anormales sur le réseau interne ont commencé le 27 octobre 2024 lorsqu'un accès non autorisé à certaines parties du réseau interne de LSC a été détecté, permettant un droit d'accès, de modification et de suppression des fichiers de LSC. Ces données incluent entre autres des numéros de sécurité sociale et des informations relatives aux banques et aux assurances.

Cela illustre les menaces persistantes à l'échelle mondiale sur les réseaux des acteurs de la santé, notamment liées à la gestion de données sensibles par ces derniers.

Source : https://www.digitaljournal.com/tech-science/over-one-million-impacted-as-laboratory-service-declares-serious-data-breach/article

UNE CYBERATTAQUE TEND UNE FOIS DE PLUS LES RELATIONS ENTRE LE MAROC ET L'ALGÉRIE

Du 13 avril 2025

La Caisse Nationale de Sécurité Sociale (CNSS) du Maroc a été la cible d'un important piratage qui a entraîné la fuite de données personnelles (numéros de carte d'identité, numéros de téléphone, coordonnées bancaires, liste d'employés de grandes entreprises) de près de deux millions de citoyens marocains.

Cette cyberattaque prend des allures de crise diplomatique entre les deux voisins maghrébins quand le porte-parole du gouvernement du royaume qualifie ces cyberattaques de « criminelle », « au timing suspect » et « une tentative de nuire aux percées diplomatiques successives du Royaume (sur le dossier du Sahara occidental, ndlr) relatives à la cause nationale », « instiguées par des parties hostiles ». En effet, le groupe associé à la cyberattaque, JabarootDZ, a diffusé sur sa chaîne Telegram les fichiers volés et prétend être un collectif nationaliste algérien. Le groupe affirme également avoir réalisé cette cyberattaque en représailles au piratage antérieur du compte Twitter de l'APS (Agence de presse algérienne), attribué à des hackers pro-marocains.

Cependant, une enquête semble indiquer que Jabaroot serait en réalité un ingénieur informatique d'origine tunisienne basé en Allemagne qui aurait exploité une zero-day encore non connue ou une faille dans un logiciel tiers utilisant des systèmes Oracle.

Source : https://www.numerama.com/cyberguerre/1949987-une-etrange-cyberattaque-tend-encore-plus-les-relations-entre-le-maroc-et-lalgerie.html

Le club cyber

elle

LE DÉBAT DE LA SEMAINE

Comment renforcer la résilience cyber des organismes de santé au niveau mondial ?

DONNE TON AVIS DANS LES COMMENTAIRES !