BULLETIN DE VEILLE N°07

ANPT-2024-BV-07

« Security used to be an inconvenience sometimes, but now it's a necessity all the time. »
- Martina Navratilova -

juillet 2024

Alertes de sécurité

Php

De multiples acteurs de la menace exploitent la faille php cve-2024-4577

11 juillet 2024

L'équipe Security Intelligence Response Team (SIRT) d'Akamai avertit que de multiples acteurs de la menace exploitent la vulnérabilité PHP CVE-2024-4577 pour diffuser plusieurs familles de logiciels malveillants, notamment Gh0st RAT, RedTail cryptominers et XMRig.

« Les acteurs de la menace ont poursuivi la tendance de la rapidité entre la divulgation et l'exploitation et ont rapidement exploité cette nouvelle vulnérabilité - nous avons observé des tentatives d'exploitation ciblant cette faille PHP sur notre réseau de pots de miel dans les 24 heures qui ont suivi sa divulgation », a rapporté Akamai.

La faille CVE-2024-4577 (score CVSS : 9.8) est une vulnérabilité d'injection de commande PHP-CGI OS. Le problème réside dans la fonction Best-Fit de la conversion d'encodage au sein du système d'exploitation Windows. Un attaquant peut exploiter cette faille pour contourner les protections d'une vulnérabilité précédente, CVE-2012-1823, en utilisant des séquences de caractères spécifiques. En conséquence, du code arbitraire peut être exécuté sur des serveurs PHP distants via une attaque par injection d'arguments, permettant aux attaquants de prendre le contrôle des serveurs vulnérables.

Depuis la divulgation de la vulnérabilité et la mise à disposition du public d'un code d'exploitation PoC, de nombreux acteurs tentent de l'exploiter, ont rapporté les chercheurs de Shadowserver et GreyNoise.

Pour Windows fonctionnant dans d'autres localités telles que l'anglais, le coréen et l'Europe de l'Ouest, en raison du large éventail de scénarios d'utilisation de PHP, il n'est actuellement pas possible d'énumérer et d'éliminer complètement tous les scénarios d'exploitation potentiels », poursuit l'avis. « Il est donc recommandé aux utilisateurs de procéder à une évaluation complète de leurs actifs, de vérifier leurs scénarios d'utilisation et de mettre à jour PHP avec la version la plus récente pour garantir la sécurité.

Source : ***https://bit.ly/3Yoo6cJ***

Docker

Vulnérabilité de contournement des plugins d'autorisation dans les plugins de Docker Engine

23 juillet 2024

Certaines versions de Docker Engine présentent une vulnérabilité de sécurité qui pourrait permettre à un attaquant de contourner les plugins d'autorisation (AuthZ) dans des circonstances spécifiques. La probabilité de base que cette vulnérabilité soit exploitée est faible. Cet avis décrit le problème, identifie les versions affectées et fournit des étapes de remédiation pour les utilisateurs concernés.

Le modèle d'autorisation par défaut de Docker est de type « tout ou rien ». Les utilisateurs ayant accès au démon Docker peuvent exécuter n'importe quelle commande Docker. Pour un meilleur contrôle d'accès, des plugins d'autorisation (AuthZ) peuvent être utilisés. Ces plugins approuvent ou refusent les demandes adressées au démon Docker en fonction de l'authentification et du contexte de la commande.

En 2018, un problème de sécurité a été découvert où un attaquant pouvait contourner les plugins AuthZ en utilisant une demande d'API spécialement conçue. Cela pourrait conduire à des actions non autorisées, y compris l'escalade des privilèges. Bien que ce problème ait été corrigé dans Docker Engine v18.09.1 en janvier 2019, la correction n'a pas été reportée sur les versions ultérieures, ce qui a entraîné une régression.

Les utilisateurs de Docker Engine v19.03.x et des versions ultérieures qui s'appuient sur des plugins d'autorisation pour prendre des décisions de contrôle d'accès sont tous concernés par cette vulnérabilité.

Aussi sans Les utilisateurs des produits commerciaux et de l'infrastructure interne de Docker qui ne s'appuient pas sur les plugins AuthZ ne sont pas affectés.

Source : ***https://bit.ly/3WMXLUy***

Actualité

Chaos et confusion : Une panne technique provoque des perturbations dans le monde entier

Les compagnies aériennes ont immobilisé leurs vols. Les opérateurs des lignes 911 n'ont pas pu répondre aux urgences. Les hôpitaux ont annulé des opérations chirurgicales. Les détaillants ont fermé pour la journée. Toutes ces actions sont dues à un lot de codes informatiques défectueux.

Une mise à jour logicielle défectueuse envoyée par une société de cybersécurité peu connue a provoqué le chaos et des perturbations dans le monde entier vendredi. L'entreprise CrowdStrike, basée à Austin, au Texas, fabrique des logiciels utilisés par des multinationales, des agences gouvernementales et de nombreuses autres organisations pour se protéger contre les pirates informatiques et les intrus en ligne.

Mais lorsque CrowdStrike a envoyé sa mise à jour jeudi à ses clients qui utilisent le logiciel Microsoft Windows, les ordinateurs ont commencé à tomber en panne.

Les retombées, immédiates et inéluctables, ont mis en évidence la fragilité de l'infrastructure technologique mondiale. Le monde est devenu dépendant de Microsoft et d'une poignée d'entreprises de cybersécurité comme CrowdStrike. Ainsi, lorsqu'un seul logiciel défectueux est diffusé sur l'internet, il peut presque instantanément endommager d'innombrables entreprises et organisations qui dépendent de cette technologie dans le cadre de leurs activités quotidiennes.

« Il s'agit d'une illustration très, très inconfortable de la fragilité de l'infrastructure centrale de l'internet dans le monde », a déclaré Ciaran Martin, ancien directeur général du National Cyber Security Center britannique et professeur à la Blavatnik School of Government de l'Université d'Oxford.

La panne généralisée n'est pas due à une cyberattaque, mais les effets de vendredi ont montré à quel point les dommages peuvent être dévastateurs lorsqu'une artère principale du système technologique mondial est perturbée. Elle a soulevé des questions plus générales sur les processus de test de CrowdStrike et sur les répercussions que devraient subir de telles sociétés de logiciels lorsque des failles dans leur code provoquent des perturbations majeures.

Si les pannes sont courantes, souvent dues à des erreurs techniques ou à des cyberattaques, l'ampleur de ce qui s'est passé vendredi est sans précédent.

« C'est historique », a déclaré Mikko Hypponen, directeur de la recherche chez WithSecure, une société spécialisée dans la cybersécurité. « Nous n'avons jamais eu d'incident de ce type.

Source: https://nyti.ms/46sJkIa

Les sites web du gouvernement de Macao sont victimes d'une cyberattaque menée par des pirates informatiques étrangers présumés

Au moins cinq sites web du gouvernement de Macao ont été mis hors ligne par des pirates informatiques étrangers présumés pendant près d'une heure en début de semaine, ont rapporté plusieurs médias chinois, citant des responsables locaux de la sécurité.

Une attaque par déni de service distribué (DDoS) a notamment touché les sites web du service de sécurité de Macao, des forces de police, des services d'incendie et de secours et de l'académie des forces de sécurité publique.

Macao est une « région administrative spéciale » située sur la côte sud de la Chine et densément peuplée. La police locale a ouvert une enquête criminelle sur ces incidents afin de remonter à la source de l'activité criminelle.

L'attaque s'est produite mercredi soir et provenait probablement « de l'étranger », selon les autorités locales.

À la suite de l'incident, les autorités de Macao ont mené une intervention d'urgence « en collaboration avec les opérateurs de télécommunications afin de rétablir rapidement les services habituels », a déclaré le secrétaire à la sécurité de la région, Wong Sio Chak.

Les forces de sécurité du pays ont également demandé à Macau Telecom, qui fournit les services permettant de bloquer les attaques DDoS, d'enquêter sur l'incident et de soumettre un rapport et un plan d'amélioration afin de prévenir des attaques similaires à l'avenir.

On ignore quel groupe de pirates informatiques est à l'origine de l'incident et quelles sont leurs motivations.

Les médias locaux ont affirmé que les dernières attaques faisaient suite à une recrudescence des cyberactivités dans la région. Selon un rapport récent, le nombre de cyberattaques visant les infrastructures critiques de Macao l'année dernière a plus que triplé depuis 2020.

Source : https://bit.ly/4fpXXAd

Bon à savoir

La fonction de partage de localisation de Snapchat peut mettre vos enfants en danger

Snapchat a annoncé une nouvelle fonctionnalité qui permet aux utilisateurs de voir où leurs amis publient sur une carte.

Malgré que cette nouvelle fonctionnalité permette de retrouver ses amis et de communiquer avec eux plus facilement que jamais, et de savoir ce que les gens font dans le monde entier, certains experts en sécurité sur internet craignent qu'elle ne soit un nouveau casse-tête pour les parents.

« D'un point de vue technique, [Snapchat] a vraiment fait son apparition, c'est une fonctionnalité super cool... mais si vous êtes parent

d'un enfant de 8 à 17 ans, c'est une tout autre paire de manches parce que c'est tellement cool et tellement interactif, et vous savez que tout le monde va s'y mettre », a déclaré Titania Jordan, responsable parentale de l'application de sécurité numérique et de solutions Bark.

Pour accéder à la nouvelle carte Snap, les utilisateurs n'ont qu'à mettre à jour leur application et il leur est demandé s'ils souhaitent accepter le partage de leur position pour tous leurs amis, pour certains d'entre eux ou s'ils choisissent de rester anonymes. Pour accéder à la mise à jour, il suffit de pincer l'appareil photo Snap pour zoomer et un monde s'ouvre, indiquant l'emplacement de vos amis. D'autres snaps, provenant de personnes non amies, s'affichent comme étant soumis à la fonction Snapchat Our Story, qui présente des vidéos et des photos sélectionnées par la communauté Snapchat.

Même si cela semble sortir de la zone du crépuscule pour les parents, la nouvelle fonctionnalité se concentre sur la technologie de partage de localisation facultative qui fait déjà partie de certains sites de médias sociaux, comme Facebook Messenger, selon Mme Jordan. Elle rappelle la fonction « Trouver mes amis » d'Apple, qui permet aux utilisateurs de trouver l'emplacement des personnes qu'ils ont contactées.

Source : ***https://bit.ly/4c7RAP6***

Evènements

Evènement à venir

ISA/IEC 62443 Cybersecurity Fundamentals Specialist 2024

5-8 Août 2024 – Online

https://bit.ly/4fu1cH2

L'Atelier virtuel ISA/IEC 62443 Cybersecurity Fundamentals Specialist s'adresse aux professionnels dans la communauté de la sécurité, le but de cet atelier est de Discuter des principes qui sous-tendent la création d'un programme efficace de sécurité à long terme, Interpréter le cadre de sécurité industrielle ISA/IEC 62443 et l'appliquer à vos activités, Définir les bases des méthodologies d'analyse des risques et des vulnérabilités, Décrire les principes de l'élaboration d'une politique de sécurité et finalement Expliquer les concepts de défense en profondeur et les modèles de sécurité par zone/conduit

Référence	ANPT-2024-BV-07
Titre	Bulletin de veille N°07
Date de version	31 juillet 2024
Contact	ssi@anpt.dz