BULLETIN DE VEILLE N°09

ANPT-2024-BV-09

"It takes 20 years to build a reputation and few minutes of cyber-incident to ruin it." – Stephane Nappo

Septembre 2024

Alertes de sécurité

Docker

CVE-2024-8695 & CVE-2024-8696 : Deux failles RCE critiques découvertes dans Docker Desktop

12 septembre 2024

Docker Desktop, l'application pour le développement d'applications conteneurisées, s'est récemment révélée présenter deux failles de sécurité critiques qui pourraient permettre des attaques par exécution de code à distance.

Docker Desktop offre aux développeurs une interface graphique rationalisée pour gérer les conteneurs, une technologie essentielle pour déployer des applications de manière cohérente dans tous les environnements. Qu'il s'agisse de tests, de développement ou de déploiement, Docker Desktop simplifie les flux de travail conteneurisés, ce qui en fait un outil indispensable pour les développeurs, même ceux qui n'ont pas de connaissances approfondies de l'infrastructure des conteneurs.

Les vulnérabilités, répertoriées comme CVE-2024-8695 et CVE-2024-8696, ont été découvertes dans les versions de Docker Desktop antérieures à 4.34.2. Elles proviennent de la façon dont Docker Desktop traite les descriptions d'extension, les journaux de modification et les URL d'éditeur. En créant des entrées malveillantes dans ces champs, les attaquants peuvent inciter Docker Desktop à exécuter du code arbitraire sur le système de la victime.

Les deux vulnérabilités ont reçu un score CVSS élevé, ce qui indique qu'elles peuvent causer des dommages importants. CVE-2024-8695 a un score CVSSv4 de 9.0, tandis que CVE-2024-8696 a un score CVSS de 8.9. Ces scores soulignent la facilité avec laquelle ces vulnérabilités peuvent être exploitées et les graves conséquences qu'elles peuvent avoir, notamment l'accès non autorisé à des données sensibles, l'installation de logiciels malveillants et la prise de contrôle complète du système affecté.

Il est essentiel que les utilisateurs prennent des mesures immédiates contre cette faille. Docker a déjà publié une version corrigée, 4.34.2, qui corrige ces vulnérabilités. Tous les utilisateurs sont vivement encouragés à mettre à jour cette version dès que possible. De plus, les utilisateurs doivent également faire preuve de prudence lorsqu'ils installent des extensions provenant de sources non fiables.

Source : ***https://bit.ly/3XUC1Wa***

Wordpress

Vulnérabilité critique d'injection SQL découverte dans le plugin WordPress 'The Events Calendar' (CVE-2024-8275)

25 Septembre 2024

Une grave faille de sécurité a été identifiée dans le populaire plugin WordPress The Events Calendar, affectant toutes les versions jusqu'à la 6.6.4 incluse. Désignée sous le nom de CVE-2024-8275, la vulnérabilité a reçu un score CVSS de 9.8, indiquant un niveau de gravité critique.

Le plugin Events Calendar, qui compte plus de 700 000 installations actives, permet aux utilisateurs de créer et de gérer facilement des calendriers d'événements sur leurs sites WordPress. Le plugin prend en charge les événements en personne et virtuels, et offre une gamme de fonctionnalités professionnelles soutenues par une équipe dévouée de développeurs et de concepteurs.

La vulnérabilité récemment découverte réside dans la fonction tribe_has_next_event(). Plus précisément, la faille est due à un escamotage insuffisant du paramètre « order » et à une préparation inadéquate des requêtes SQL existantes. Cet oubli permet à des attaquants non authentifiés de réaliser des attaques par injection SQL en ajoutant des requêtes SQL supplémentaires. L'exploitation de cette vulnérabilité pourrait permettre à des attaquants d'extraire des informations sensibles de la base de données, ce qui pourrait compromettre l'intégrité du site et les données des utilisateurs.

Il est important de noter que seuls les sites ayant ajouté manuellement la fonction tribe_has_next_event() sont vulnérables à cette faille d'injection SQL. Toutefois, étant donné l'utilisation répandue de cette fonction par les développeurs qui personnalisent leurs calendriers d'événements, le risque reste important.

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

Actualité

Plus de 44 millions de dollars en crypto-monnaie volés sur la plateforme singapourienne BingX

La plateforme cryptographique singapourienne BingX a déclaré vendredi que plus de 44 millions de dollars avaient été volés lors d'une cyberattaque.

Les entreprises spécialisées dans la sécurité de la blockchain ont commencé à voir des millions sortir de la plateforme jeudi soir avant que l'entreprise ne publie un message sur les médias sociaux concernant une fermeture liée à la « maintenance des portefeuilles ». La société a rapidement publié une déclaration plus longue disant que la perturbation a été déclenchée après que la société ait « détecté un accès anormal au réseau, indiquant potentiellement une attaque de pirates informatiques sur le hot wallet de BingX. »

« Nous avons immédiatement mis en œuvre des mesures d'urgence, y compris le transfert urgent d'actifs et la suspension temporaire des retraits. Il y a eu une perte mineure d'actifs, mais le montant est faible et est en cours de calcul », ont-ils déclaré. Ils ont ajouté que seule une « petite quantité » de fonds est conservée directement sur la plateforme pour répondre aux demandes de retrait. Les retraits ont été interrompus à la suite de l'attaque.

La société a ensuite publié un audit plus complet avec l'aide de la société de sécurité de la blockchain SlowMist, qui a déclaré avoir suivi jusqu'à présent environ 44,7 millions de dollars de pertes. D'autres entreprises ont déclaré que les pertes pourraient atteindre 48 millions de dollars, mais BingX a admis qu'elle était encore en train de calculer le montant qui a été dérobé.

« Bien que la perte soit encore en cours de calcul, nous confirmons ce qui suit : BingX compensera entièrement la perte avec son propre capital. La perte totale est minime et gérable », a déclaré Vivien Lin, chef de produit chez BingX.

« Cet incident n'affectera pas nos opérations commerciales en cours. Les services de négociation se poursuivent comme d'habitude. Les retraits et les dépôts sont temporairement retardés et devraient être rétablis dans les 24 heures au plus tard. »

L'attaque contre BingX intervient alors que plusieurs plateformes cryptographiques basées en Asie ont été confrontées à des incidents de sécurité financièrement préjudiciables cette année. La plus grande plateforme cryptographique d'Indonésie s'est vu dérober 20 millions de dollars la semaine dernière, tandis qu'une autre plateforme cryptographique de Singapour, Penpie, a signalé la semaine dernière un incident au cours duquel 27 millions de dollars ont été dérobés.

Des plateformes en Inde et au Japon ont perdu respectivement plus de 230 millions et 300 millions de dollars lors d'attaques en début d'année.

Source : https://bit.ly/3Bre6pC

Une cyberattaque massive a touché la Banque centrale d'Iran et d'autres banques iraniennes

Iran International rapporte qu'une cyberattaque massive a perturbé les opérations de la Banque centrale d'Iran (CBI) et de plusieurs autres banques du pays. L'attaque a paralysé les systèmes informatiques des banques du pays.

Cet incident coïncide avec l'intensification de la surveillance internationale des opérations de l'Iran au Moyen-Orient, Téhéran ayant annoncé des attaques contre Israël à moins d'un cessez-le-feu dans le conflit de Gaza. Les experts du renseignement accusent également l'Iran de tenter d'influencer les prochaines élections présidentielles américaines.

Selon Iran International, il s'agit de l'une des plus importantes cyberattaques contre l'infrastructure de l'État iranien à ce jour.

Plus tôt dans la journée de mercredi, le guide suprême iranien, l'ayatollah Ali Khamenei, a déclaré que « l'exagération des capacités de nos ennemis est destinée à répandre la peur parmi notre peuple par les États-Unis, la Grande-Bretagne et les sionistes. La main de l'ennemi n'est pas aussi forte qu'on le dit. Nous devons compter sur nous-mêmes. L'objectif de l'ennemi est de répandre la guerre psychologique pour nous faire reculer politiquement et économiquement et atteindre ses objectifs. »

« Cette cyberattaque survient à un moment où les actions de l'Iran dans la région font l'objet d'une surveillance internationale accrue, l'Iran ayant promis de riposter à l'assassinat du chef du Hamas, Ismail Haniyeh, au début du mois. Les dirigeants du Royaume-Uni, de la France et de l'Allemagne ont publié une déclaration commune avertissant l'Iran qu'il « portera la responsabilité » de toute attaque contre Israël, ce qui pourrait aggraver les tensions régionales et compromettre les efforts déployés en vue d'un cessez-le-feu et d'un accord sur la libération des otages », a rapporté le site web israélien Israel Hayom.

Les dirigeants européens ont exhorté l'Iran et ses alliés à éviter de nouvelles attaques afin d'éviter une nouvelle escalade entre Israël et le Hamas.

Source : https://bit.ly/3yQCDnf

Bon à savoir

Soyez prudent lorsque vous vous connectez à un wifi public.

Les réseaux Wi-Fi publics, bien que pratiques, peuvent représenter un risque majeur pour la cybersécurité s'ils ne sont pas utilisés avec précaution. Ces réseaux sont souvent non sécurisés, ce qui permet aux cybercriminels d'intercepter plus facilement les données qui transitent entre votre appareil et l'internet. Lorsque vous vous connectez à un réseau Wi-Fi public, vos activités en ligne, y compris la navigation, l'envoi de courriels et la saisie de mots de passe, peuvent être exposées à des acteurs malveillants par le biais d'une technique appelée « attaque de l'homme du milieu ». Les pirates peuvent mettre en place de faux points d'accès

Wi-Fi qui semblent légitimes, vous incitant à vous connecter et à transmettre des informations sensibles. Pour réduire les risques, évitez d'effectuer des activités sensibles telles que des opérations bancaires en ligne, des achats ou l'accès à des fichiers liés au travail lorsque vous utilisez un réseau Wi-Fi public. Si vous devez accéder à des informations sensibles, il est essentiel d'utiliser un réseau privé virtuel (VPN). Un VPN crypte votre connexion internet, ce qui rend l'espionnage de vos activités beaucoup plus difficile. En outre, veillez à désactiver les connexions automatiques aux réseaux Wi-Fi dans les paramètres de votre appareil et ne vous connectez qu'aux réseaux auxquels vous faites confiance. Vérifiez toujours le nom du réseau auprès de l'établissement proposant le Wi-Fi afin d'éviter les points d'accès falsifiés ou malveillants. En faisant attention à la manière dont vous utilisez le Wi-Fi public et au moment où vous l'utilisez, vous pouvez mieux protéger vos données personnelles contre les cybermenaces.

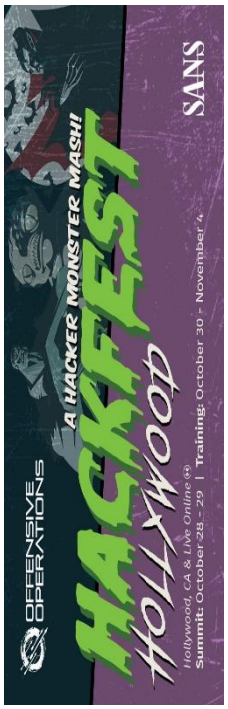
Evènements

Evènement à venir

SANS HackFest Hollywood 2024

28 octobre/ 4 novembre - Online

https://www.sans.org/



Si les films de monstres nous ont appris quelque chose, c'est que le danger est toujours au coin de la rue. Au HackFest Hollywood, les praticiens les plus offensifs de la cybersécurité partagent les tactiques effrayantes et effrayées utilisées par les adversaires d'aujourd'hui.

Ce sommet de deux jours couvre tous les aspects de l'aspect offensif de la cybersécurité. Qu'il s'agisse de tests de pénétration, d'émulation d'adversaires, d'exploitation ou d'équipes d'intervention, des conférences, des ateliers, des CTF et d'autres surprises effrayantes vous attendent. Ce sera une convergence inoubliable de piratage et d'horreur, qui vous permettra d'être mieux équipé pour protéger votre organisation contre les monstres qui se cachent dans l'ombre numérique.

Référence	ANPT-2024-BV-09
Titre	Bulletin de veille N°09
Date de version	30 septembre 2024
Contact	ssi@anpt.dz