BULLETIN DE VEILLE N°12

ANPT-2020-BV-12

« L'un des tests du leadership est la capacité de reconnaître un problème avant qu'il ne devienne une urgence. » - *Arnold H. Glasow-*

Décembre 2020

Alertes de sécurité

HPE

HPE dévoile un zero-day critique dans son logiciel de gestion de serveur

16 décembre 2020

Hewlett Packard Enterprise (HPE) a révélé un bug zero-day référencé CVE-2020-7200 dans les dernières versions (7.6.x.) de son logiciel propriétaire HPE Systems Insight Manager (SIM) pour Windows et Linux.

La vulnérabilité résulte du manque de validation appropriée des données fournies par l'utilisateur, elle peut être exploitée par des attaquants sans privilèges pour exécuter du code à distance sur des serveurs exécutant la version vulnérable de son logiciel SIM.

Bien que les mises à jour de sécurité ne soient pas encore disponibles pour cette vulnérabilité d'exécution de code à distance (RCE), HPE a fourni des informations d'atténuation Windows et travaille sur la résolution du bug.

Dans son bulletin de sécurité, l'entreprise a expliqué que la vulnérabilité peut être atténuée en désactivant les fonctionnalités «Recherche fédérée» et «Configuration CMS fédérée» de SIM.

Source : *https://bit.ly/2J7auy8*

Cisco

Cisco corrige les vulnérabilités de Security Manager avec des exploits publics

07 décembre 2020

Cisco a publié des mises à jour de sécurité pour résoudre plusieurs vulnérabilités d'exécution de code à distance pré-authentification avec des exploits publics affectant Cisco Security Manager (CSM).

Les vulnérabilités ont été signalées par Florian Hauser, chercheur en sécurité chez Code White. Le chercheur a également publié des exploits de preuve de concept pour les 12 vulnérabilités de Cisco Security Manager, car Cisco PSIRT a cessé de répondre à ses demandes.

Un attaquant distant et non authentifié pourrait exploiter les failles pour exécuter des commandes arbitraires sur les appareils concernés.

Cisco a corrigé les failles avec la publication de CSM version 4.22 Service Pack 1.

Source : *http://bit.ly/3rjNQ71*

Microsoft

PoC publié pour la vulnérabilité Windows non corrigée présente depuis 2006

11 décembre 2020

Des détails et un exploit de preuve de concept (PoC) ont été publiés pour une vulnérabilité d'escale de privilèges non corrigée dans Windows liée à l'outil d'administration PsExec.

La vulnérabilité a été découverte par le chercheur de Tenable, David Wells, et elle a été révélée cette semaine après que Microsoft n'ait pas réussi à publier un correctif dans les 90 jours.

Microsoft n'a pas dit quand ou si cette vulnérabilité sera corrigée, mais le géant de la technologie a souligné que «cette technique nécessite qu'un attaquant ait déjà compromis la machine cible pour exécuter du code malveillant.»

La vulnérabilité est un problème d'escale de privilèges local qui peut être exploité par un processus non administrateur pour élever les privilèges à SYSTEM lorsque PsExec est exécuté à distance ou localement sur l'ordinateur cible.

Il a été constaté que la faille de sécurité avait un impact sur les versions de Windows entre Windows XP et Windows 10, et les versions de PsExec entre 2.2 (la dernière) et 1.7.2 (sortie en 2006).

Un article a été publié contenant des détails techniques et un exploit PoC a été rendu disponible sur GitHub.

Source : *http://bit.ly/37H0DZD*

Google révèle un bug Windows 0-Day mal corrigé, maintenant non corrigé

24 décembre 2020

Google a rendu public les détails d'une vulnérabilité de sécurité zero-day mal corrigée dans l'API du spouleur d'impression Windows qui pourrait être exploitée par un acteur malveillant pour exécuter du code arbitraire.

La faille référencée CVE-2020-0986 concerne une élévation de privilège dans le GDI Print / Spouleur d'impression API ("splwow64.exe") qui a été signalée à Microsoft par un utilisateur anonyme travaillant avec Zero Day Initiative (ZDI) de Trend Micro fin décembre 2019.

Une exploitation réussie de cette vulnérabilité pourrait amener un attaquant à manipuler la mémoire du processus "splwow64.exe" pour exécuter du code arbitraire en mode noyau, l'utilisant finalement pour installer des programmes malveillants ; afficher, modifier ou supprimer des données ; ou créer de nouveaux comptes avec tous les droits d'utilisateur.

Bien que Microsoft ait finalement adressé la faille dans le cadre de sa mise à jour de juin Patch Tuesday, de nouvelles découvertes de l'équipe de sécurité de Google révèlent que elle n'a pas été entièrement corrigée.

Source : *http://bit.ly/37RCM9G*

Apache

Apache Software Foundation corrige une faille d'exécution de code dans Apache Struts 2

09 décembre 2020

La faille d'exécution de code à distance, référencée CVE-2020-17530, peut être déclenchée lorsqu'un acteur malveillant envoie une expression OGNL (Object-Graph Navigation Language) malveillante qui peut entraîner une exécution de code à distance dans le contexte de l'application Struts 2 affectée.

Selon les privilèges associés à l'application affectée, un attaquant pourrait effectuer plusieurs activités malveillantes, telles que l'installation d'applications ; modifier ou supprimer des données, ou créer de nouveaux comptes administrateur.

La faille affecte Struts 2.0.0 à Struts 2.5.25 et a été corrigée avec la sortie de Struts 2.5.26.

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

WordPress

Vulnérabilité dans Formulaire de contact 7 touche +5 millions de sites

17 décembre 2020

Une vulnérabilité sérieuse a été corrigée dans le formulaire de contact 7 qui permet aux attaquants de charger des scripts malveillants.

La vulnérabilité référencée CVE-2020-35489 permet à un adversaire non authentifié de prendre le contrôle d'un site Web exécutant le plugin ou éventuellement de détourner l'ensemble du serveur hébergeant le site. Le correctif se présente sous la forme d'une mise à jour de la version 5.3.2 du plugin Contact Form 7.

Une description plus détaillée de la vulnérabilité a été publiée sur la page de dépôt du plugin WordPress de Contact Form 7.

Toutes les versions du formulaire de contact 7 à partir de 7 5.3.1 et moins sont considérées comme vulnérables et doivent être mises à jour immédiatement.

Source : *http://bit.ly/3nGG3y1*

Kubernetes

Une vulnérabilité Kubernetes Man-in-the-Middle non résolue

21 décembre 2020

Le 4 décembre 2020, le comité de sécurité des produits Kubernetes a révélé une nouvelle vulnérabilité Kubernetes attribuée à CVE-2020-8554. Il s'agit d'un problème de gravité moyenne affectant toutes les versions de Kubernetes et qui n'est actuellement pas corrigé. CVE-2020-8554 est une faille de conception qui permet aux services Kubernetes d'intercepter le trafic du cluster vers n'importe quelle adresse IP. Les utilisateurs qui peuvent gérer les services peuvent exploiter la vulnérabilité pour mener des attaques de type «man-in-the-middle» (MITM) contre les pods et les nœuds du cluster.

Le comité de sécurité des produits Kubernetes a déterminé que la correction de la vulnérabilité CVE-2020-8554 entraînerait des changements dans plusieurs fonctionnalités de Kubernetes, il n'est donc pas prévu de résoudre la vulnérabilité à court terme. Au lieu de cela, le comité a recommandé plusieurs mesures d'atténuation qui limitent l'accès aux fonctionnalités vulnérables, soit sur la base d'un contrôleur d'admission personnalisé, soit par le biais d'une règle de gate-keeper de l'Open Policy Agent (OPA) .

Source : *http://bit.ly/2JaYD24*

Google

CERT-IN avertit les utilisateurs en Inde de mettre à jour immédiatement le navigateur Google Chrome

08 décembre 2020

Google a récemment publié l'une des plus importantes mises à jour du navigateur Chrome - Chrome 87 - qui corrige les principales vulnérabilités de sécurité et CERT-IN conseille tous les utilisateurs d'obtenir la dernière version de Google Chrome - version 87.0.4280.88 […].

CERT-IN a également expliqué que cette mise à jour Chrome est une prévention contre l'accès et/ou le vol d'informations personnelles par les pirates informatiques.

"Un attaquant pourrait exploiter ces vulnérabilités en persuadant une victime de visiter un site Web spécialement conçu. Une exploitation réussie de ces vulnérabilités pourrait permettre à l'attaquant d'exécuter du code arbitraire, d'accéder à des informations sensibles ou de contourner les restrictions de sécurité sur le système ciblé" […].

La nouvelle version 87 de Chrome a été optimisée pour consommer moins de batterie en mettant en veille les onglets et processus inactifs.

Source : *http://bit.ly/38m8OcM*

Actualité

Le piratage de la chaîne d'approvisionnement SolarWinds : ce que vous devez savoir

18 Décembre 2020

Des pirates informatiques, présumés russes, ont réussi à pénétrer par effraction dans les systèmes d'informations des départements gouvernementaux clés et ont eu accès aux e-mails internes […].

Les cyberattaques étaient «hautement sophistiquées», les pirates ont réussi à contourner le logiciel de sécurité Microsoft utilisé par la National Telecommunications and Information Administration.

Les attaquants ont obtenu l'accès aux e-mails internes des départements du Trésor et du Commerce dans le cadre d'une attaque qui a également ciblé plusieurs autres départements gouvernementaux et agences de sécurité nationales, a rapporté The New York Times.

Les attaques étaient en cours depuis le printemps (mars). Selon plusieurs rapports, les hackers auraient fait irruption en exploitant les mises à jour de SolarWind, une société informatique utilisée par le gouvernement et l'armée américains pour gérer les réseaux.

Les pirates qui semblent être associés au groupe de piratage Cozy Bear, alias Advanced Persistent Threat (APT) group 29, qui fait partie de la branche SVR des services de renseignement russes, se sont infiltrés dans les opérations de développement de SolarWinds et ont réussi à insérer des logiciels malveillants dans une mise à jour qui a été distribuée par l'entreprise en mars. Une fois installé, le logiciel malveillant contacte un réseau de commande et de contrôle géré par le groupe de piratage, ce qui leur a permis de s'infiltrer dans le réseau et d'apporter d'autres mesures. Vu que le correctif provenait de l'entreprise et avait été signé numériquement par SolarWinds, peu de sociétés se sont rendu compte que leur logiciel était compromis jusqu'à présent.

Il est important de mentionner que tous les clients de SolarWinds ne sont pas vulnérables à ce hack, et que ce dernier concerne seulement les utilisateurs de la plateforme logicielle Orion ainsi que ceux qui ont chargé la mise à jour de mars. D'après SolarWinds, le nombre de clients dotés de cette mise à jour est aux alentours de 18 000.

Source : *http://bit.ly/3nCXtLR*

Exfiltration de données à partir d'un ordinateur Air-gap via des signaux WI-FI

14 décembre 2020

Un chercheur en sécurité a démontré que les données sensibles pouvaient être exfiltrées à partir d'ordinateurs Air-gap via une nouvelle technique qui exploite les signaux Wi-Fi comme un canal secret - étonnamment, sans nécessiter la présence de matériel Wi-Fi sur les systèmes ciblés.

Surnommée « AIR-FI », l'attaque repose sur le déploiement d'un malware spécialement conçu dans un système compromis qui exploite «les bus DDR SDRAM pour générer des émissions électromagnétiques dans les bandes Wi-Fi 2,4 GHz» et la transmission d'informations sur ces fréquences qui peuvent ensuite être interceptées et décodées par des appareils compatibles Wi-Fi à proximité tels que les smartphones, les ordinateurs portables et les appareils IoT avant d'envoyer les données à des serveurs distants contrôlés par un attaquant […].

Les nouvelles recherches rappellent encore une fois que les composants électromagnétiques, acoustiques, thermiques et optiques continuent d'être des vecteurs lucratifs pour monter des attaques d'exfiltration sophistiquées contre différentes installations.

Source : *http://bit.ly/2KLT5vf*

Plus de la moitié des organisations n'ont pas de plan de réponse aux risques internes

15 décembre 2020

Selon un rapport de Code42, tant les chefs d'entreprise que les responsables de la sécurité permettent à d'énormes problèmes de risque interne de s'aggraver à la suite du passage important au travail à distance au cours de l'année écoulée.

Au cours de cette période, 76% des responsables de la sécurité informatique ont déclaré que leurs organisations avaient subi une ou plusieurs violations de données, impliquant la perte de fichiers sensibles, principalement en raison des utilisateurs ayant accès aux fichiers qu'ils ne devraient pas. Malgré ces forces, 54% n'ont toujours pas de plan pour répondre aux risques internes.

Avant la pandémie, les technologies de collaboration basées sur le cloud et la mobilité de la main-d'œuvre étaient devenues les principaux moteurs de l'exfiltration des données, car les programmes d'atténuation des risques ne parvenaient pas à suivre le rythme du lieu de travail numérique actuel […].

Les exigences de productivité nécessitent l'utilisation d'outils permettant la rapidité et la collaboration entre les organisations, mais les équipes de sécurité sont largement limitées dans leur capacité à surveiller ces outils pour détecter les comportements à risque en raison d'une dépendance excessive aux technologies de blocage traditionnelles.

Les équipes de sécurité n'ont pas le bon contexte pour le problème et continuent à déployer des technologies qui bloquent le partage de fichiers, ce qui a inévitablement un impact sur la productivité des employés et des équipes de sécurité. En même temps que les tendances autour du travail à distance devraient se poursuivre, le budget des programmes de gestion des risques internes demeure un sujet de préoccupation.

Source : *http://bit.ly/3mAdbWF*

Vulnérabilité cPanel et WHM facile à exploiter avec les informations d'identification Dark Web

15 décembre 2020

Les plates-formes d'hébergement Web telles que cPanel et WebHost Manager (WHM) sont des cibles de choix pour les cybercriminels. Les logiciels malveillants sophistiqués ne sont plus nécessaires pour accéder à ces plates-formes d'hébergement Web. Au lieu de cela, les cybercriminels peuvent exploiter une vulnérabilité d'authentification à deux facteurs (2FA) récemment révélée en utilisant des informations d'identification valides, qui peuvent facilement être achetées sur les marchés du dark web.

Le 24 novembre 2020, les chercheurs de Digital Defense ont révélé une vulnérabilité affectant la suite logicielle cPanel et WHM utilisée par les clients pour gérer plus de 70 millions de domaines dans le monde. Sur la base des résultats, une vulnérabilité 2FA a été trouvée dans cPanel et WHM version 11.90.0.5 (90.0 Build 5) qui permettait aux attaquants de contourner la sécurité des comptes, ce qui pouvait conduire à la prise de contrôle des domaines de la cible. Pour exploiter avec succès cette faille, les attaquants auraient besoin des informations d'identification valides de la cible, qui peuvent être obtenues soit par l'utilisation d'attaques de phishing, soit par l'achat d'informations d'identification cPanel auprès d'une tierce source. Les organisations les plus exposées à ces exploits sont celles qui n'ont pas corrigé cette vulnérabilité et qui n'effectuent pas de veille sur les différents forums et marchés tierces.

Source *: http://bit.ly/2WyleJ3*

Trois millions d'utilisateurs ont installé 28 extensions malveillantes Chrome ou Edge

17 décembre 2020

Plus de trois millions d'internautes auraient installé 15 extensions Chrome et 13 extensions Edge contenant du code malveillant, a déclaré la société de sécurité Avast.

Les 28 extensions contenaient du code qui pouvait effectuer plusieurs opérations malveillantes. Avast a déclaré avoir trouvé du code pour :

- Rediriger le trafic utilisateur vers les annonces
- Rediriger le trafic des utilisateurs vers les sites de phishing
- Collecter des données personnelles, telles que les dates de naissance, les adresses e-mail et les appareils actifs
- Recueillir l'historique de navigation
- Télécharger d'autres logiciels malveillants sur l'appareil d'un utilisateur

Mais malgré la présence de code pour alimenter toutes les fonctionnalités malveillantes ci-dessus, les chercheurs d'Avast ont déclaré qu'ils pensaient que l'objectif principal de cette campagne était de détourner le trafic des utilisateurs pour des gains monétaires […].

Jusqu'à ce que Google ou Microsoft terminent leurs enquêtes et décident de leur plan d'action, Avast a recommandé aux utilisateurs de désinstaller et de supprimer les extensions de leurs navigateurs (Voir la source).

Source *: http://zd.net/3h821ay*

Les cybercriminels lancent une vague d'attaques sur des sites Wordpress vulnérables

27 novembre 2020

Lors d'un incident découvert récemment, un nouveau gang de cybercriminalité a exploité des sites WordPress vulnérables pour installer des magasins de commerce électronique frauduleux dans le but de réduire le classement et la réputation d'un site dans les moteurs de recherche.

Les attaquants ont eu accès au compte administrateur du site grâce à des attaques par force brute, après quoi ils ont écrasé le fichier d'index principal du site et ont ajouté du code malveillant.

Les chercheurs ont également découvert que des attaquants injectaient des fichiers PHP malveillants dans les sites WordPress pour assurer un flux constant de liens de spam SEO.

[…] Il n'est pas surprenant que des vulnérabilités non corrigées dans les logiciels de base de WordPress alimentent les ambitions malveillantes des cyberattaquants. Par conséquent, traiter les problèmes de sécurité au bon moment et suivre les meilleures pratiques de cybersécurité est une réponse pour sécuriser les sites WordPress contre les cyberattaques.

Source *: https://bit.ly/36hk4Ho*

Bon à savoir !

Ces derniers temps, nous avons été témoins d'un intérêt croissant pour l'utilisation des VPN (Virtual Private Network). Un VPN crypte le trafic Internet de l'utilisateur et l'achemine via des serveurs distants, protégeant ses données (comme l'historique de navigation, les téléchargements et les messages de chat) et masquant aussi son emplacement.

Beaucoup d'utilisateurs connaissent les atouts du VPN, mais ne se rendent pas compte que ce dernier s'accompagne de quelques points négatifs. Parmi ces derniers, nous citons :

- Le fournisseur VPN peut voir tout votre trafic et en faire ce qu'il veut, y compris la journalisation.
- Dans la plupart des cas, les VPN font très peu pour améliorer la sécurité ou la confidentialité de vos données à moins d'être associés à d'autres changements.

- Agir comme ils le font et promouvoir les fournisseurs de VPN commerciaux comme solution aux problèmes potentiels faits plus de mal que de bien.

Les points ci-dessus concernent les VPN payants et gratuits, et la situation est encore plus critique concernant les VPN gratuits.

Le seul cas de figure où vous serez dans l'obligation d'utiliser un VPN est lorsque vous êtes sur un réseau connu comme hostile (par exemple, un point d'accès WiFi d'aéroport public, ou un FAI connu pour utiliser MITM), et vous souhaitez contourner ce problème. En effet, le risque de se connecter à un réseau public est plus grand que de se connecter via un service VPN.

Il est à rappeler que l'utilisation de ce type d'outils dans le réseau de l'agence est interdite afin d'assurer un maximum de protection pour le réseau et les données y transitant.

Evènements

Evènements du mois

Sommet du leadership exécutif du CIO des services financiers

10 Décembre 2020, Online

http://bit.ly/2WKEhQy

L'événement virtuel de HMG a permis aux les leaders de la sécurité dans les services financiers - les hauts dirigeants de la technologie- de partager leurs conseils sur les rôles que les DSI et les leaders technologiques peuvent jouer dans l'innovation et la refonte de l'avenir du travail.

Le sommet aide les DSI, RSSI et autres responsables technologiques à assurer le succès de leurs entreprises et de tirer parti de leurs expériences passées et actuelles dans la crise actuelle mais aussi d'appliquer un nouvel état d'esprit pour faire avancer l'entreprise vers un avenir meilleur avec courage et compassion.

Conférence internationale sur la cybersécurité et les systèmes d'information sécurisés (ICCSIS) 2020

21-22 Décembre 2020, Istanbul, Turquie

http://bit.ly/38CUWLi

La Conférence internationale sur la cybersécurité et les systèmes d'information sécurisés a rassemblé des scientifiques universitaires et des chercheurs pour échanger et partager leurs expériences et leurs résultats de recherche sur tous les aspects de la cybersécurité et des systèmes d'information sécurisés. Il a offert également une plateforme interdisciplinaire de premier ordre aux chercheurs, praticiens et éducateurs pour présenter et discuter des innovations, tendances et préoccupations les plus récentes, ainsi que des défis pratiques rencontrés et des solutions adoptées dans les domaines de la cybersécurité et des systèmes d'information sécurisés.

La conférence a sollicité des contributions de résumés, d'articles et d'affiches électroniques qui traitent des thèmes et des sujets de la conférence, y compris des figures, des tableaux et des références de nouveaux matériaux de recherche.

Evènements à venir

Le sommet IoT du pétrole et du gaz

20-21 Janviers 2021, Lisbonne, Portugal.

http://bit.ly/3pu9rYF

Le Oil and Gas IoT Summit rassemble une communauté exclusive d'environ 120 parties prenantes majeures provenant d'opérateurs mondiaux, d'EPC, de régulateurs et de fournisseurs de technologies pour débattre et discuter des principales questions et tendances qui façonnent la transformation numérique de l'industrie.

En se concentrant sur les preuves d'études de cas et les leçons apprises, les conférenciers partageront leurs expériences personnelles, leurs défis et leurs résultats RÉELS. En gardant un œil sur l'avenir, l'évènement présentera également les principales tendances et évolutions qui devraient façonner l'industrie au cours des 12 prochains mois et au-delà.

Reference	ANPT-2020-BV-12
Titre	Bulletin de veille N°12
Date de version	31 Décembre 2020
Contact	ssi@anpt.dz