BULLETIN DE VEILLE N°05

ANPT-2022-BV-05

"Plutôt que de craindre ou d'ignorer les cyberattaques, assurez-vous de votre cyber-résilience."
— Stephane Nappo --

Mai 2022

Alertes de sécurité

Microsoft

Un bogue Zero-Day affecte toutes les versions Windows

10 Mai 2022

Microsoft a corrigé une vulnérabilité de type Zero-Day d'usurpation d'identité LSA (Local Security Authority) de Windows activement exploité, permettant aux attaquants non authentifiés de forcer les contrôleurs de domaine à les authentifier via le protocole de sécurité Windows NT LAN Manager (NTLM).

Suivie sous le nom de CVE-2022-26925, la faille a été exploitée dans la nature et semble être liée à l'attaque PetitPotam de relais NTLM.

Grâce à ce nouveau vecteur d'attaque, les acteurs de la menace peuvent intercepter des demandes d'authentification légitimes qui peuvent être utilisées pour une escalade des privilèges, permettant probablement la compromission complète du domaine.

Les attaquants ne peuvent abuser de cette faille que dans le cadre d'attaques man-in-the-middle (MITM) très complexes, où ils doivent être en mesure d'intercepter le trafic entre la victime et un contrôleur de domaine pour lire ou modifier les communications réseau.

Microsoft a corrigé ce bogue qui affecte toute les versions de Windows ainsi que deux autres, un bogue de déni de service de Windows Hyper-V (CVE-2022-22713) et une faille du pilote ODBC Magnitude Simba Amazon Redshift (CVE-2022-29972), dans le cadre du Patch Tuesday de mai 2022.

Source : *https://bit.ly/3Mc6aZh*

Android

36 correctifs dans le Patch de Mai 2022 d'Android

05 Mai 2022

Dans le cadre des mises à jour de sécurité de mai 2022 pour Android, Google a publié des correctifs pour 36 vulnérabilités, dont une qui semble avoir été exploitée.

La plus grave de ces failles de sécurité est un problème de haute gravité dans le composant Framework d'Android qui pourrait être exploité pour une escalade de privilèges.

Elle a été résolue en même temps que quatre autres vulnérabilités dans Framework, dont trois bogues d'élévation de privilèges de gravité élevée et un problème de divulgation d'informations de gravité moyenne.

Les correctifs résolvent également huit vulnérabilités dans le composant System, toutes ont été classées de gravité élevée (trois bogues conduisent à une élévation de privilèges, trois à une divulgation d'informations et deux à un déni de service).

Parmi les autres corrections inclus dans ses mises à jour, 04 bogues dans les composants du noyau, 03 problèmes dans les composants MediaTek, 05 dans les composants Qualcomm, et 11 dans les composants Qualcomm à code source fermé.

Il est toujours recommandé de mettre à jour les systèmes vulnérables vers des versions plus fiables afin d'atténuer tout risque possible.

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

Zoom

Un correctif pour le logiciel de vidéoconférence Zoom

25 Mai 2022

Le chercheur Ivan Fratric a révélé une chaîne d'exploitation qui peut être utilisée par un acteur malveillant pour compromettre un utilisateur de Zoom via la fonction de chat - sans interaction de l'utilisateur - en lui envoyant un message via le protocole XMPP. Une partie de la chaîne d'exploitation de Fratric a été baptisée "XMPP Stanza Smuggling".

Fratric a décrit un total de six vulnérabilités. Deux des failles, identifiées comme CVE-2022-25235 et CVE-2022-25236, ont un impact sur le célèbre analyseur XML open source Expat.

Comme cette bibliothèque est utilisée dans de nombreux projets, plusieurs grands fournisseurs ont publié des avis pour informer leurs clients de l'impact de ces vulnérabilités et

d'autres vulnérabilités d'Expat, notamment IBM, Aruba, diverses distributions Linux, Oracle et F5.

Les vulnérabilités spécifiques à Zoom trouvées par Fratric ont été décrites par Zoom comme des problèmes de haute et moyenne gravité liés à une analyse XML incorrecte (CVE-2022-22784), au déclassement des paquets de mise à jour (CVE-2022-22786), à une validation insuffisante du nom d'hôte (CVE-2022-22787) et à des cookies de session incorrectement contraints (CVE-2022-22785).

CVE-2022-22786 affecte Zoom Client for Meetings pour Windows et Zoom Rooms for Conference Room pour Windows. Les autres affectent Zoom Client for Meetings sur toutes les plateformes de bureau et mobiles.

Les utilisateurs de Zoom sont invités à mettre à jour leurs clients à la version 5.10.0 afin de corriger ces vulnérabilités.

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

dotCMS

Une faille RCE critique affecte le logiciel de gestion de contenu dotCMS

04 Mai 2022

Une vulnérabilité critique a été découverte dans le système de gestion de contenu open-source 'dotCMS'.

Suivie sous le nom de CVE-2022-26352, la faille provient d'une attaque par traversée de répertoire lors du téléchargement de fichiers, permettant à un adversaire pré-authentifié d'exécuter des commandes arbitraires sur le système vulnérable.

"Un attaquant peut télécharger des fichiers arbitraires sur le système", a déclaré Shubham Shah d'Assetnote dans un rapport. "En téléchargeant un fichier JSP dans le répertoire racine du tomcat, il est possible d'obtenir une exécution de code, ce qui conduit à l'exécution de commandes."

En d'autres termes, la faille de téléchargement de fichiers arbitraires peut être utilisée de manière abusive pour remplacer des fichiers déjà existants dans le système par un shell web, qui peut ensuite être utilisé pour obtenir un accès distant persistant.

Des correctifs ont été publiés dans les versions 22.03, 5.3.8.10 et 21.06.7, ce qui permet aux utilisateurs d'atténuer les risques possibles en appliquant ces mises à jour.

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

F5

F5 met en garde ses clients BIG-IP contre 18 vulnérabilités sévères

04 Mai 2022

F5 a publié une notification de sécurité trimestrielle pour informer leurs clients sur plus de 50 vulnérabilités affectant les contrôleurs de livraison d'applications BIG-IP, dont une considérée comme critique et 17 classées comme étant de haute gravité.

La faille critique, découverte en interne par F5, est répertoriée sous le nom de CVE-2022-1388 et peut être exploitée par un attaquant non authentifié disposant d'un accès réseau à un système BIG-IP pour exécuter des commandes système arbitraires, créer ou supprimer des fichiers ou désactiver des services. Le problème affecte le composant REST d'iControl et il a été décrit comme un "problème de plan de contrôle" qui n'implique aucune exposition du plan de données.

Trois des vulnérabilités de haute gravité ont reçu un score CVSS compris entre 8 et 9. Deux d'entre elles, CVE-2022-25946 et CVE-2022-27806, affectent les systèmes fonctionnant en "mode appliance" et permettent à un attaquant authentifié disposant de privilèges d'administrateur de contourner les restrictions spécifiques à ce mode.

Le troisième problème, CVE-2022-28707, est une vulnérabilité XSS (cross-site scripting) qui peut être exploitée pour l'exécution de code JavaScript arbitraire par un attaquant qui a accès au système avec au moins les privilèges "guest".

Il est recommandé d'affecter les correctifs dès que possible car les acteurs de la menace sont connus pour cibler les vulnérabilités affectant le produit BIG-IP.

Source : *https://bit.ly/3a6zBOE*

Avast et AVG

Deux failles vieilles de 10ans affectent les antivirus Avast et AVG

05 Mai 2022

Deux vulnérabilités de sécurité de haute gravité ont été découvertes dans un pilote utilisé par les solutions antivirus Avast et AVG, elles peuvent permettre à un attaquant d'élever ses privilèges et éventuellement désactiver les solutions antivirus.

Les failles, identifiées comme CVE-2022-26522 et CVE-2022-26523, se trouvent dans le pilote de noyau anti-rootkit nommé aswArPot.sys qui est le "Avast anti-rootkit", signé numériquement par AVAST Software. Le pilote a été introduit dans la version 12.1 d'Avast, qui date de juin 2012.

"SentinelLabs a découvert deux failles de haute gravité dans Avast et AVG (acquis par Avast en 2016) qui sont restées non découvertes pendant 10 ans, affectant des dizaines de millions d'utilisateurs", indique l'avis publié par SentinelOne. "Ces vulnérabilités permettent aux attaquants d'élever leurs privilèges, ce qui leur permet de désactiver des produits de sécurité, d'écraser des composants système, de corrompre le système d'exploitation ou d'effectuer des opérations malveillantes sans entrave."

Les chercheurs ont indiqué que la plupart des installations d'Avast et d'AVG seront automatiquement mises à jour, tandis que, il est recommandé d'appliquer les correctifs manuellement sur les installations en mode air ou sur site.

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

Actualité

Des malwares cachés dans les journaux des événements de Windows

Les chercheurs de Kaspersky ont remarqué une campagne malveillante qui utilisait les journaux d'événements de Windows pour stocker des logiciels malveillants, une technique qui n'avait pas été documentée publiquement auparavant pour des attaques dans la nature.

Les chercheurs ont collecté un échantillon du malware et ont trouvé que l'une des parties les plus intéressantes de l'attaque consiste à injecter des charges utiles de shellcode dans les journaux d'événements Windows pour les services de gestion des clés (KMS), une action réalisée par un dropper de malware personnalisé.

La nouvelle technique analysée par Kaspersky est probablement en passe de devenir plus populaire, car le code source permettant d'injecter des charges utiles dans les journaux d'événements de Windows a été disponible dans l'espace public pendant une brève période.

Parmi les outils utilisés dans l'attaque figurent les cadres commerciaux de tests de pénétration Cobalt Strike et NetSPI.

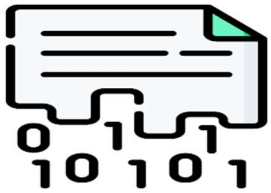
En étudiant l'attaque, Kaspersky n'a trouvé aucune similitude avec des campagnes précédentes associées à un acteur de menace connu.

Jusqu'à ce qu'un lien avec un adversaire connu soit établi, les chercheurs suivent cette nouvelle activité sous le nom de SilentBreak, d'après le nom de l'outil le plus utilisé dans l'attaque.

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

Des sites Web transmettent les données des courriels des utilisateurs à des domaines de suivi du Web

Dans le cadre d'une enquête sur la manière dont les données des formulaires en ligne sont utilisées pour le suivi, une équipe de quatre informaticiens a mesuré l'ampleur de la collecte des adresses électroniques et des mots de passe avant l'envoi des formulaires en analysant les 100 000 principaux sites web.



L'équipe a constaté que les adresses électroniques étaient exfiltrées vers des domaines de suivi avant la soumission du formulaire et sans consentement sur 1 844 sites Web dans le crawl de l'UE et 2 950 sites Web dans le crawl des États-Unis.

Dans la majorité des cas, les données ont été extraites vers des domaines de suivi bien connus, mais les chercheurs ont également identifié 41 domaines de suivi omis des listes de blocage populaires.

Les internautes saisissent généralement leur adresse électronique dans des formulaires en ligne, notamment pour s'inscrire à un service ou s'abonner à une lettre d'information.

"Certains sites Web ont dit qu'ils ne savaient pas que les e-mails de leurs visiteurs étaient collectés par des tiers, et ils ont corrigé le problème", a déclaré Gunes Acar, l'un des quatre principaux chercheurs.

Les internautes soucieux de leur vie privée pourraient bien reculer devant ces révélations, résumées dans un billet de blog contenant des captures d'écran et des vidéos.

Afin de se protéger Acar conseille d'adopter certaines contre-mesures : "Les bloqueurs de publicité et les navigateurs axés sur la protection de la vie privée peuvent empêcher ce type de collecte de données.

"Les services de relais de messagerie peuvent être utilisés pour éviter de donner la même adresse électronique à différentes entreprises en ligne et hors ligne. Apple, DuckDuckGo et Mozilla proposent de tels services, qui peuvent être utilisés pour générer des adresses alias", conclut Acer.

***Source :** https://bit.ly/3NFunI7*

Une augmentation massive de l'activité des logiciels malveillants Linux XorDDoS

Microsoft a révélé que le logiciel malveillant XorDDoS qui utilisé pour pirater les appareils Linux et construire un botnet DDoS, a connu une augmentation massive de 254% de son activité au cours des six derniers mois.

XorDDoS est connu pour cibler une multitude d'architectures système Linux, de ARM (IoT) à x64 (serveurs), et compromettre celles qui sont vulnérables dans des attaques SSH par force brute.

Pour se propager à davantage de dispositifs, il utilise un script shell qui tentera de se connecter en tant que root en utilisant divers mots de passe contre des milliers de systèmes exposés à Internet jusqu'à ce qu'il trouve finalement une correspondance.

En plus de lancer des attaques DDoS, les opérateurs du malware utilisent le botnet XorDDoS pour installer des rootkits, maintenir l'accès aux appareils piratés et, probablement, déposer des charges utiles malveillantes supplémentaires.

"Nous avons constaté que les appareils d'abord infectés par XorDdos étaient ensuite infectés par d'autres logiciels malveillants tels que la porte dérobée Tsunami, qui déploie en outre le monnayeur XMRig", ajoute Microsoft.

L'augmentation considérable de l'activité de XorDDoS détectée par Microsoft depuis décembre correspond à un rapport de la société de cybersécurité CrowdStrike, selon lequel les logiciels malveillants Linux ont connu une croissance de 35 % en 2021 par rapport à l'année précédente.

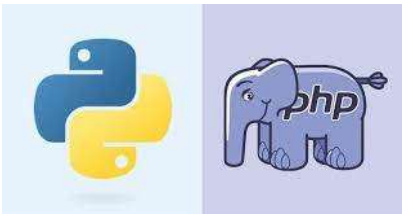
XorDDoS, Mirai et Mozi étaient les familles les plus répandues, représentant 22 % de toutes les attaques de logiciels malveillants ciblant les appareils Linux observées en 2021.

Parmi les trois, CrowdStrike a déclaré que XorDDoS a connu une augmentation notable de 123 % d'une année sur l'autre, tandis que Mozi a connu une croissance explosive de son activité, avec dix fois plus d'échantillons détectés dans la nature tout au long de l'année dernière.

Source : *https://bit.ly/38lklNr*

Des bibliothèques PyPI et PHP détournés !

Deux librairies Python et PHP trojanisés ont été découverts dans ce qui constitue un nouvel exemple d'attaque de la chaîne d'approvisionnement logicielle visant l'écosystème open source.



L'une des librairies en question est "ctx", un module Python disponible dans le dépôt PyPi. L'autre implique "phpass", une librairie PHP qui a été bifurqué sur GitHub pour distribuer une mise à jour malveillante.

"Dans les deux cas, l'attaquant semble avoir pris le contrôle des librairies qui n'ont pas été mis à jour depuis un certain temps", a déclaré le SANS Internet Storm Center (ISC).

On soupçonne que l'attaquant a réussi à obtenir un accès non autorisé au compte du mainteneur pour publier la nouvelle version de ctx. Une enquête plus approfondie a révélé que l'acteur de la menace a enregistré le domaine expiré utilisé par le responsable original le 14 mai 2022.

"Avec le contrôle du nom de domaine original, la création d'une adresse électronique correspondante pour recevoir un courriel de réinitialisation de mot de passe serait triviale", a ajouté Ching. "Après avoir obtenu l'accès au compte, l'auteur pourrait supprimer l'ancien librairie et télécharger les nouvelles versions rétrogradées."

"On dirait que la compromission de phpass s'est produite parce que le propriétaire du librairie source - 'hautelook' - a supprimé son compte et que l'attaquant a revendiqué le nom d'utilisateur", a déclaré le chercheur indépendant Somdev Sangwan dans une série de tweets, détaillant ce que l'on appelle une attaque de détournement de dépôt.

Les dépôts publics de code open source tels que Maven, NPM, Packages, PyPi et RubyGems constituent une partie essentielle de la chaîne d'approvisionnement en logiciels sur laquelle de nombreuses organisations s'appuient pour développer des applications.

D'un autre côté, cela en fait également une cible attrayante pour divers adversaires qui cherchent à diffuser des logiciels malveillants.

Source : https://bit.ly/38lklNr

Cloud… soyons prêts

S'adapter au changement après la migration vers le Cloud

Après la migration vers le cloud, les entreprises doivent être prêtes pour s'adapter à certains changements. Pour cela, il est important de prendre en considération les aspects suivants :

La formation : Si le cloud modifie les responsabilités de l'équipe informatique, il ne les élimine pas. Il est important donc de former l'équipe informatique afin d'assurer qu'elle sait quelles sont les tâches dont elle reste responsable et en quoi elles diffèrent dans le cloud. Outre la formation de l'équipe d'exploitation, les équipes de développement doivent comprendre comment l'utilisation du cloud modifie la façon dont elles conçoivent, construisent, testent et déploient leurs applications.

Le suivi : La surveillance des machines virtuelles, des ressources du système d'exploitation et de la disponibilité des applications doit être une tache continue afin de pouvoir détecter les moindres problèmes dès leurs apparition et s'assurer que les utilisateurs finaux bénéficient de performances adéquates. De même, il faut disposer d'une surveillance axée sur les questions de sécurité et de conformité juridique et réglementaire, étant donné que la sécurité est une responsabilité partagée entre l'entreprise et le fournisseur Cloud.

La réactivité et la gestion d'incidents : Dans les mois/années qui suivent la migration vers le Cloud, il y aura surement une panne, un problème de performance, une perte de données et/ou une faille de sécurité, etc. C'est pourquoi il est primordial d'avoir une stratégie bien organisée pour ces incidents intégrant des personnes formées, des processus définis et de la technologie nécessaires afin de pouvoir se remettre rapidement des incidents, déployer rapidement un correctif et atténuer le problème sans avoir un impact négatif sur l'expérience des clients, des partenaires ou des employés.

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

Bon à savoir !

La gestion de vulnérabilités, comment procéder ?

Edgescan, le fournisseur de solutions de gestion intelligente des vulnérabilités, a publié les conclusions de son rapport 2022 sur les statistiques des vulnérabilités, qui, pour la septième année consécutive, offre une vue d'ensemble de l'état de la gestion des vulnérabilités dans le monde.

Le rapport révèle que les organisations prennent encore près de deux mois pour remédier aux vulnérabilités à risque critique, le délai moyen de remédiation (MTTR) sur l'ensemble de la pile étant de 60 jours.

Etant donné que plus une vulnérabilité reste longtemps dans la nature, plus un attaquant a le temps de préparer un exploit, le fait de ne pas se tenir régulièrement à jour des rustines peut entraîner des résultats désastreux pour les organisations.

Voici donc cinq conseils pour assurer une bonne gestion des correctifs et éliminer le risque d'exploitation :

- **Connaître ses responsabilités :** Il convient tout d'abord de déterminer ses cibles et où elles se trouvent : les postes de travail, serveurs, applications et services pour lesquels le service informatique a la responsabilité des correctifs en constante évolution.
- **Des procédures différenciées selon l'urgence** : Une stratégie d'entreprise de gestion des correctifs devrait comporter deux procédures : la procédure standard et la procédure d'urgence. La première détaille les processus d'application régulière des mises à jour planifiées. Ce calendrier permet de créer un rythme suivant avec lequel travailler de manière régulière et éviter que l'application des mises à jour prenne du retard. Tandis que la seconde procédure concerne les cas où des correctifs doivent être appliqués d'urgence. Pour cela, il convient de déterminer avec grand soin les seuils devant être atteints pour ouvrir une fenêtre de maintenance d'urgence.
- **Suivre les chronologies de distribution de correctifs :** Le nombre de systèmes d'exploitation, d'applications ou encore de firmwares présents dans l'environnement varie considérablement d'une organisation à l'autre, tout comme les calendriers de distribution de mises à jour des éditeurs et constructeurs concernés. Par exemple, Microsoft diffuse les siens de manière mensuelle, avec son *Patch Tuesday*. Il est nécessaire de tenir compte de ces chronologies dans le cadre des procédures normales d'application de correctifs, ainsi que dans les procédures d'urgence.
- **Concevoir et maintenir un environnement de test réaliste :** Un environnement de test des correctifs et mises à jour vise à établir l'impact d'un patch dans l'environnement de production. Il est nécessaire de s'accorder suffisamment de temps pour tester effectivement les nouveaux correctifs avant leur déploiement.
- **Examiner les processus et leurs résultats :** Une fois qu'un correctif a été appliqué avec succès, il convient de revenir sur le processus pour identifier les points d'amélioration potentiels, et faire évoluer les procédures en conséquence.

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

Evènements

Evènement du mois

Hack.INI

26-28 Mai 2022

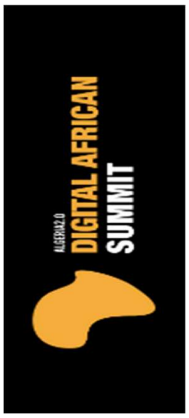
ESI, Oued Smar, Alger

https://bit.ly/38swm3I

Le club de cyber sécurité Shellmate a organisé l'évènement Hack.IINI qui est destiné aux passionnées du domaine de la cyber sécurité.

Cet évènement s'est déroulé en trois jours durant lesquelles une compétition Capture The Flag (CTF) a été organisée ainsi qu'un ensemble d'ateliers traitant plusieurs thématiques du domaine comme le Digital Forensics et la sécurité du Docker.

Evènement à venir



Digital African Summit

31 Mai – 02 Juin 2022

CIC d'Alger

https://bit.ly/3wXAhOk

Digital African Summit est un évènement qui réunit les acteurs du secteur du digital Africain dans le but d'envisager l'édification de projets futuristes sur le continent et ailleurs dans le monde. Au cours de cet évènement, il y aura des expositions de plus de 200 entreprises et startups, 60 conférences, workshops et discours des grands acteurs, des compétitions de pitch de startup, des réunions B2B, ainsi que des sessions de networkings et des expositions culturelles et touristiques.

Référence	ANPT-2022-BV-05
Titre	Bulletin de veille N°05
Date de version	31 Mai 2022
Contact	ssi@anpt.dz