BULLETIN DE VEILLE N°09

ANPT-2021-BV-09

« Alors que le monde est de plus en plus interconnecté, tout le monde partage la responsabilité de sécuriser le cyberspace. » -Newton Lee-

Septembre 2021

Alertes de sécurité

Chrome

Mise à jour d'urgence !

24 Septembre 2021

Google a publié la version Chrome 94.0.4606.61 pour Windows, Mac et Linux, une mise à jour d'urgence qui corrige une vulnérabilité Zero-Day de haute gravité exploitée dans la nature.

Le bug, suivi sous le nom de CVE-2021-37973, est une faiblesse de type "use after free" dans Portals, le nouveau système de navigation des pages web de Google pour Chrome. Son exploitation peut permettre aux attaquants d'exécuter du code arbitraire sur des ordinateurs utilisant des versions non corrigées de Chrome.

Afin de prévenir les tentatives d'exploitation, les utilisateurs sont invités à vérifier manuellement la présence de nouvelles mises à jour dans le menu Chrome > Aide > À propos de Google Chrome, et le navigateur mettra automatiquement à jour après le prochain lancement.

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

Apple

Trois vulnérabilités Zero-Day dans les appareils Apple, l'une permet l'installation de Peagasus !

2021

Apple a publié des mises à jour de sécurité pour corriger trois Zero-Days ce mois-ci. Les deux premières sont enregistrées sous les noms CVE-2021-30860 et CVE-2021-30858. Toutes deux permettent à des documents malveillants d'exécuter des commandes lorsqu'ils sont ouverts sur des appareils vulnérables.

Citizen Lab a confirmé que CVE-2021-30860 est un exploit iMessage de type zero-day zero-click nommé "FORCEDENTRY" qui est utilisé pour contourner la fonction de sécurité iOS BlastDoor afin de déployer le logiciel espion NSO Pegasus sur des appareils appartenant à des activistes bahreïnis.

La troisième vulnérabilité se trouve dans le Finder de macOS. Elle permet aux attaquants d'exécuter des commandes arbitraires sur des Mac exécutant toute version de macOS jusqu'à la dernière, Big Sur.

Bien qu'Apple ait corrigé le problème sans attribuer de numéro d'identification CVE, ce correctif reste incomplet car il peut être contourné, selon l'avis de SSD Secure Disclosure.

Source : *https://bit.ly/2XSg91Y*

Cisco

Cisco corrige des problèmes de sécurité très critiques dans IOS XE

02 Septembre 2021

Cisco a publié des correctifs pour corriger trois vulnérabilités de sécurité critiques dans son système d'exploitation de réseau IOS XE.

La première, CVE-2021-34770, est une vulnérabilité d'exécution de code à distance CAPWAP dans le logiciel Cisco IOS XE pour les contrôleurs sans fil de la famille Catalyst 9000 (score CVSS : 10.0).

La seconde est un problème de dépassement de tampon dans le logiciel Cisco IOS XE SD-WAN (score CVSS : 9.8).

L'autre faille, CVE-2021-1619, est une vulnérabilité de contournement d'authentification NETCONF et RESTCONF dans le logiciel Cisco IOS XE (score CVSS : 9.8).

"Une exploitation réussie pourrait permettre à l'attaquant d'exécuter du code arbitraire avec des privilèges administratifs ou de provoquer le verrouillage et le rechargement du périphérique affecté, ce qui entraînerait une condition de DoS." indique la société dans son avis.

Cisco a également corrigé 15 vulnérabilités de gravité élevée et 15 de gravité moyenne affectant divers composants du logiciel

IOS XE ainsi que la plate-forme de points d'accès Cisco et le logiciel Cisco SD-WAN vManage. Il est conseillé aux utilisateurs et aux administrateurs d'appliquer les mises à jour nécessaires afin d'atténuer tout risque d'exploitation par des acteurs malveillants.

Source : *https://bit.ly/3a92bE3*

Microsoft

Une nouvelle vulnérabilité Zero-Day très grave dans Ms office 365

14 Septembre 2021

Microsoft a corrigé une vulnérabilité zero-day de haute gravité activement exploitée dans des attaques ciblées contre Microsoft Office et Office 365 sur des ordinateurs Windows 10.

La faille d'exécution de code à distance (RCE), suivie sous le nom de CVE-2021-40444, a été découverte dans le moteur de rendu du navigateur Internet Explorer MSHTML utilisé par les documents Microsoft Office.

Les attaques ciblées détectées par Microsoft ont tenté d'exploiter la vulnérabilité en envoyant à des victimes potentielles des documents Office spécialement conçus contenant des contrôles ActiveX malveillants.

Microsoft a publié un avis détaillant la vulnérabilité ainsi que les systèmes affectés.

"Veuillez consulter le tableau des mises à jour de sécurité pour connaître la mise à jour applicable à votre système. Nous vous recommandons d'installer ces mises à jour immédiatement.", a déclaré la société.

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

Patch Tuesday de Microsoft

14 Septembre 2021

Dans le Patch Tuesday de ce mois, Microsoft a corrigé 60 vulnérabilités (86 en comptant Microsoft Edge) dont deux de type Zero-day.

Parmi ces vulnérabilités, nous trouvons :

- 27 vulnérabilités d'élévation de privilège ;
- 16 vulnérabilités d'exécution de code à distance ;
- 11 vulnérabilités de divulgation d'informations ;
- 8 vulnérabilités d'usurpation d'identité.
- 2 vulnérabilités de contournement des fonctions de sécurité. ;
- 1 vulnérabilité de déni de service ;

Les deux Zero-day corrigées sont celle d'exécution de code à distance de Windows MSHTML (CVE-2021-40444) et une vulnérabilité d'élévation de privilège Windows DNS (CVE-2021-36968).

Pour plus d'informations sur la description complète de chaque vulnérabilité et des systèmes qu'elle affecte, vous pouvez consulter ce rapport.

Source *: https://bit.ly/39GthKr*

VMware

Des failles dans vCenter Server et Cloud Foundation

21 Septembre 2021

VMware a signalé l'existence de plusieurs vulnérabilités dans les appliances vCenter Server et Cloud Foundation qu'un attaquant distant pourrait exploiter pour prendre le contrôle du système affecté.

La plus grave d'entre elles est une vulnérabilité de téléchargement de fichier arbitraire dans le service Analytics (CVE-2021-22005) qui impacte les déploiements de vCenter Server 6.7 et 7.0, avec un code d'exploitation disponible publiquement que les attaquants utilisent déjà.
Cette faille peut être utilisée par toute personne pouvant atteindre vCenter Server sur le réseau pour obtenir un accès, quels que soient les paramètres de configuration de vCenter Server.
18 autres vulnérabilités ont été identifiées, nous citons :

- CVE-2021-21991 (score CVSS : 8.8) : Vulnérabilité d'élévation de privilèges locaux.
- CVE-2021-22013 (Score CVSS : 7.5) : Vulnérabilité de traversée de chemin de fichier (File traversal).
- CVE-2021-21992 (Score CVSS : 6.5) : Vulnérabilité de déni de service de l'analyse XML.

Les autres vulnérabilités sont listées dans l'avis de VMware. Il est vivement recommandé de rester vigilant et d'appliquer les correctifs publiés.

Sources *: https://bit.ly/39ELmsn*

Netgear

Les routeurs et les commutateurs intelligents exposés à de nouveaux problèmes de sécurité

06-21 Septembre 2021

Netgear a publié des correctifs pour remédier à trois vulnérabilités de sécurité affectant ses commutateurs intelligents. Ces vulnérabilités peuvent être utilisées par un attaquant pour prendre le contrôle total d'un appareil vulnérable.
Les failles concernent un détournement de l'authentification et une vulnérabilité qui pourrait permettre à un attaquant de modifier le mot de passe de l'administrateur sans avoir à connaître le mot de passe précédent ou de détourner les informations de démarrage de la session, ce qui entraînerait une compromission totale du dispositif.
De plus, l'entreprise a corrigé une vulnérabilité d'exécution de code à distance affectant plusieurs routeurs, répertoriée CVE-2021-40847. Elle pourrait être exploitée par des attaquants distants pour prendre le contrôle d'un système affecté.
Face à la nature critique des vulnérabilités, il est recommandé aux entreprises qui utilisent les commutateurs Netgear concernés de passer à la dernière version dès que possible afin d'atténuer tout risque d'exploitation.

Sources : *https://bit.ly/3EWw8Nx*
https://bit.ly/3zIVxXu

Toutes les alertes de sécurité du mois de septembre peuvent être consultées sur notre application mobile NATP NEWS

Actualité

Bitcoin.org: le Giveaway frauduleux

24 Septembre 2021

Le site Web Bitcoin.org a été mis hors service aux premières heures de la matinée du 23 septembre après sa compromission par des tiers qui ont affiché des messages pop-up promettant aux visiteurs du site de doubler leur argent en envoyant des fonds vers un portefeuille bitcoin. Le message indiquait que les 10 000 premiers visiteurs de Bitcoin.org à envoyer des bitcoins (à l'adresse de l'escroc) en recevraient le double. Le message comprenait un code QR et l'adresse du porte-monnaie des fraudeurs. Les visiteurs étaient incapables de quitter la fenêtre contextuelle.

L'attaque semble provenir de l'exploitation d'une faille dans le DNS du site. Les escrocs ont accumulé plus de 17 000 dollars de bitcoins en 10 transactions.

Bien que la situation soit à présent sous contrôle et que le site semble fonctionner normalement, il faut reconnaître que le mal est fait.

***Sources** : https://bit.ly/3AJSmzY, https://bit.ly/39HZWPJ*

Une nouvelle version du malware JUPYTER se distribue à travers l'installateur MSI

21 Septembre 2021

Jupyter, apparu la première fois en 2020, est un backdoor basé .NET qui cible principalement les données des navigateurs Chromium, Firefox et Chrome. Et depuis, Jupyter est resté actif et très évasif. Il a continué à être très faiblement détecté voir pas du tout détecté sur VirusTotal, ce qui présume sa capacité à contourner les solutions de détection.

Le 8 septembre 2021, une nouvelle chaîne de diffusion du backdoor qui passe sous le radar des solutions de sécurité a été identifiée montrant ainsi que le malware n'a pas seulement continué à être actif, mais aussi que les acteurs de la menace ne cessent de développer leurs attaques pour devenir plus efficaces et plus évasifs.

La nouvelle chaîne de livraison a fait usage d'une application PDF appelée Nitro Pro. Les attaques commencent par le déploiement d'un fichier d'installation MSI de plus de 100 Mo, ce qui permet de contourner les moteurs anti-malware, et obscurci à l'aide d'un assistant de conditionnement d'applications tiers appelé Advanced Installer. L'exécution de la charge utile MSI conduit à l'exécution d'un loader PowerShell intégré dans un binaire légitime de Nitro Pro 13, dont deux variantes ont été observées signées avec un certificat valide appartenant à une entreprise réelle en Pologne, ce qui suggère une possible usurpation ou vol de certificat. Le loader, dans la phase finale, décode et exécute le module .NET Jupyter en mémoire.

L'évolution continuelle de ce type de logiciel les rendant de plus en plus performant, nous incite à être plus vigilants quant à la sécurité de nos informations.

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

Chainsaw : Un nouvel analyseur d'évènements Windows

06 Septembre 2021

F-Secure a mis en open source un nouvel outil pour les équipes de réponse aux incidents et professionnels de la cybersécurité, appelé Chainsaw, conçu pour identifier rapidement les menaces dans les journaux d'événements Windows.

Chainsaw offre une méthode générique et rapide de recherche de mots-clés dans les journaux d'événements, et d'identification des menaces à l'aide d'une logique de détection intégrée et via la prise en charge des règles de détection Sigma. Écrit en Rust et accessible par ligne de commande, il devrait être particulièrement utile aux équipes IR et Blue Team qui répondent aux incidents de sécurité. Chainsaw est disponible sur GitHub.

***Source** : https://bit.ly/3ANMi9v*

Nouvelle escroquerie avec le nom de « Elon Musk »

19 Septembre 2021

Les arnaqueurs utilisent des spams par e-mail pour promouvoir un nouveau concours. Cette nouvelle escroquerie sur le thème d'Elon Musk s'appelle "Elon Musk Mutual Aid Fund" ou "Elon Musk Club".

Les e-mails contiennent une pièce jointe HTML intitulée "Get Free Bitcoin - [id].htm" ou "Elon Musk Club - [id].htm", qui ne contient qu'une ligne de code. Le code inclus dans les pièces jointes utilise JavaScript afin de rediriger le navigateur vers la page Web *https://msto.me/elonmusk/*.

Après que les victimes aient rempli de multiples formulaires sur la page web, ils seront envoyés vers une page finale indiquant qu'ils doivent d'abord faire un don de 0,001 bitcoins à un autre utilisateur pour pouvoir recevoir "l'aide financière". Par conséquent, tout le monde doit savoir que presque tous les sites de dons de crypto-monnaies sont des canulars, en particulier ceux qui se font passer pour Elon Musk, Tesla, SpaceX ou Gemini.

Si vous recevez des courriels, des tweets ou d'autres messages sur les médias sociaux faisant la promotion d'offres similaires, il est probablement prudent de supposer que les bitcoins que vous donnerez ne seront pas remboursés.

Source : *https://bit.ly/39Q6bAV*

Twitter introduit une nouvelle fonctionnalité contre les comportements abusifs

01 Septembre 2021

Le harcèlement et d'autres formes de comportement abusif sur les médias sociaux sont devenus un problème récurrent, et les plateformes de médias sociaux s'efforcent de l'éradiquer depuis quelque temps déjà.

Twitter a dévoilé une nouvelle fonctionnalité appelée "Safety Mode", qui vise à réduire les comportements abusifs en bloquant automatiquement les tweets indésirables et autres formes de harcèlement en ligne. Pour l'instant, cette fonctionnalité n'est disponible que pour une poignée d'utilisateurs.

Lorsque la fonction Mode sécurité est activée, elle bloque brièvement, pour une période de sept jours, les comptes qui utilisent un langage injurieux tel que des insultes ou des commentaires répugnants, ainsi que ceux qui envoient des mentions répétitives ou non sollicitées.

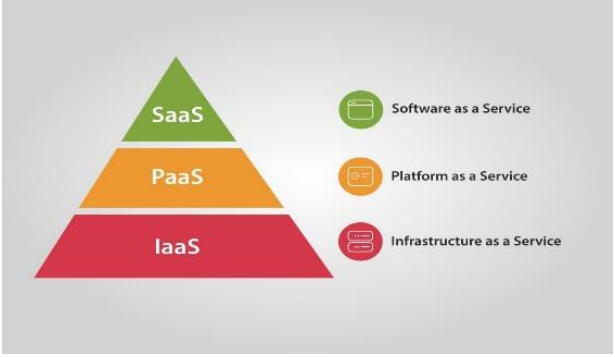
Source : *https://bit.ly/39KOe76*

Cloud… soyons prêts !

IaaS, PaaS et SaaS, Que choisir ?

IaaS, PaaS et SaaS sont les trois principaux types d'offres de services Cloud :

- IaaS, ou infrastructure en tant que service, est un accès à la demande aux serveurs physiques et virtuels, au stockage et à la mise en réseau. Son principal avantage est le fait qu'il permet aux clients d'éviter les dépenses initiales liés à l'achat et à la maintenance de leurs Data Centers et élimine le compromis entre le gaspillage lié à l'achat d'une capacité excédentaire sur site pour faire face aux pics de trafic.
- PaaS, ou platform as a service, est un accès à la demande à une plateforme complète. Il permet aux clients de créer, tester, déployer, exécuter, mettre à jour et mettre à l'échelle des applications plus rapidement et à moindre coût que s'ils devaient créer et gérer leur propre plate-forme sur site.
- SaaS, ou software as a service, est un accès à la demande à un logiciel d'application prêt à l'emploi, hébergé dans le cloud. Son principal avantage est qu'il permet de décharger toute la gestion de l'infrastructure et des applications sur le fournisseur du SaaS.



La solution as-a-service qu'un client choisit doit dépendre principalement de la fonctionnalité dont il a besoin et de l'expertise dont il dispose au sein de son personnel. Par exemple, une entreprise qui ne dispose pas de l'expertise informatique interne pour configurer et exploiter des serveurs distants n'est pas bien adaptée à l'IaaS.

Mais dans certains cas, les trois modèles constituent une solution viable. Dans ces cas, les entreprises comparent les alternatives en fonction de la facilité de gestion qu'elles offrent et au besoin en termes de sécurité par rapport au contrôle qu'elles abandonnent par la migration vers le cloud.

Source : *https://ibm.co/2ZEQQBC*

Bon à savoir !

Phishing : Prévention et bonnes pratiques

Les campagnes de phishing continuent de tromper même les plus vigilants d'entre nous, c'est l'un des risques de sécurité les plus courants et sous-estimés auxquels les professionnels de l'informatique sont confrontés.

C'est une technique utilisée par les attaquants pour obtenir des informations personnelles ou professionnelles et déployer des malwares. Les fraudeurs ont recours à différents moyens pour inciter les gens à se connecter à leurs liens et à leur donner les informations qu'ils veulent.

Étant donné que cette attaque cible le facteur humain, il reste toujours imprédictible. Pour cette cause les organisations et les individus doivent être conscient du danger que ça représente et des bonnes pratiques à appliquer afin de se protéger. Parmi ces pratiques nous citons :

- Ne fournissez jamais vos informations personnelles en réponse à une demande non sollicitée, que ce soit par téléphone ou sur Internet ;
- Si vous pensez que le contact peut être légitime, contactez vous-même l'expéditeur. S'il s'agit d'une institution ou d'une entreprise, vous pouvez trouver ses coordonnées sur l'internet ;
- Ne donnez jamais votre mot de passe par téléphone ou en réponse à une demande non sollicitée sur Internet ;
- Ne fournissez jamais d'informations financières personnelles, notamment votre numéro de sécurité sociale, vos numéros de compte ou vos mots de passe ;
- Ne vous laissez pas intimider par un courriel ou un appel qui vous suggère des conséquences terribles si vous ne fournissez pas ou ne vérifiez pas immédiatement des informations financières ;
- Protégez vos comptes en utilisant une authentification multifactorielle ;
- Ne vous laissez pas tenter par des pop-ups ;
- Filtrez vos e-mails.

Si vous êtes victime d'une attaque, agissez immédiatement pour vous protéger. Et Signalez les courriels ou appels suspects à votre supérieur hiérarchique.

***Sources** : https://bit.ly/2Wvitvv ; https://bit.ly/3i2ZoZM*

Evènements

Evènements du mois

La cybersécurité pour les responsables de sécurité

29 Septembre 2021

Online

https://bit.ly/3AQgXmG

Le webinaire "Better Security, Better Care" en collaboration avec le Centre national de cybersécurité, du Centre de cyber-résilience (SW) et du Forum national sur les soins, ont organisés une session de mise à jour et de soutien pratique sur la façon de réduire et de gérer les cyberattaques.
Plusieurs sujets ont été abordés et développés au cours de cette session concernant les cyber-attaques et leurs risques, ils ont également donné des consignes pratiques sur la manière dont on peut réduire le risque d'une cyberattaque, et la façon de répondre en cas d'attaque.

Evènements à venir

Le CTF national de cybersécurité en Algérie 2021

02 Octobre 2021

Online

https://bit.ly/3ifC6iT

En coopération avec Trend Micro, en tant que partenaire stratégique, CyberTalents organise son 3ème CTF national de cybersécurité en Algérie.

Le CTF sera en style Jeopardy où chaque équipe aura une liste de défis dans différentes catégories comme Reverse Engineering, Web Security, Digital Forensics, Network Security et autres. L'équipe qui obtiendra le meilleur score à la fin sera l'équipe gagnante, et pourra participer aux CTF régionales et internationales en représentant l'Algérie.

Référence	ANPT-2021-BV-09
Titre	Bulletin de veille N°09
Date de version	30 Septembre 2021
Contact	ssi@anpt.dz