BULLETIN DE VEILLE N°05

ANPT-2021-BV-05

«Security is not a product but a process » **Bruce Schneier-**

Mai 2021

Alertes de sécurit

Microsoft

Microsoft met fin à Internet Explorer

11 mai 2021

Microsoft a publié des mises à jour pour corriger 55 failles de sécurité dans ses systèmes d'exploitation Windows et d'autres logiciels. Quatre de ces vulnérabilités peuvent être exploitées par un tiers malveillant pour prendre le contrôle total et à distance des systèmes vulnérables sans aucune intervention des utilisateurs. La vulnérabilité la plus critique ce mois-ci est la CVE-2021-31166 , une faille Windows 10 et Windows Server qui permet à un attaquant non authentifié d'exécuter à distance un code malveillant au niveau du système d'exploitation.

Une autre vulnérabilité référencée CVE-2021-26419 de corruption de mémoire existe dans Microsoft Internet Explorer. Une exploitation réussie de cette vulnérabilité pourrait permettre à un attaquant distant d'exécuter du code arbitraire sur le système affecté. La société de Redmond a annoncé que le 15 juin 2022, l'application de bureau Internet Explorer 11 sera « retirée et ne sera plus supportée ».

Il est toujours recommandé pour les utilisateurs de Windows de mettre à jour leurs systèmes au moins une fois par mois, dès que ces dernières sont stables.

Source *: https://bit.ly/34kaEJy*

Publication du PoC pour la vulnérabilité Wormable du serveurWindows IIS

19 mai 2021

Une analyse et une preuve de concept (Poc) ont été partagées pour une vulnérabilité de serveur Windows IIS « wormable» qui pourrait avoir une exploitation de code potentielle. Microsoft a suivi cela dans un correctif déclaré CVE-2021-31166 .

La faille pourrait être exploitée par un attaquant non authentifié en envoyant un paquet spécialement conçu à un serveur ciblé utilisant la pile du protocole HTTP (http.sys) pour traiter les paquets.

Ce code d'exploitation PoC provoque le crash d'un système Windows non patché exécutant un serveur IIS, il n'implémente pas les capacités de vermifuge. Les attaquants pourraient amorcer l'exploitation de la vulnérabilité dans la nature, le code PoC pourrait être amélioré pour être activement exploité.

Le correctif CVE-2021-31166 publié récemment par Microsoft corrige le bug spécifié ci-dessus qui pourrait permettre à un attaquant non authentifié d'exécuter du code à distance en tant que système. À noter que Windows 10 peut également être configuré en tant que serveur Web, il est donc également impacté.

Source *: https://bit.ly/3c3hxmR*

Adobe

Adobe Reader : une vulnérabilité 0-day exploitée

13 mai 2021

Selon Adobe, une vulnérabilité critique zero-day est activement exploitée dans la nature qui affecte son logiciel de lecture Adobe Acrobat PDF omniprésent.

La vulnérabilité référencée CVE-2021-28550 affecte huit versions du logiciel, y compris celles exécutées sur les systèmes Windows et macOS. Ces versions comprennent :

Windows Acrobat DC & Reader DC (versions 2021.001.20150 et antérieures), macOS Acrobat DC & Reader DC (versions 2021.001.20149 et antérieures), Windows et macOS Acrobat 2020 et Acrobat Reader 2020 (2020.001.30020 et versions antérieures), Windows et macOS Acrobat 2017 et Acrobat Reader 2017 (2017.011.30194 et versions antérieures).

«Les utilisateurs sont invités à mettre à jour manuellement les installations de leurs produits en choisissant Aide> Rechercher les mises à jour».

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

Pulse Connect Secure VPN

Nouvelle vulnérabilité de haute gravité signalée dans Pulse Connect Secure VPN

25 mai 2021

Ivanti, la compagnie propriétaire des appliances Pulse Secure VPN, a publié un avis de sécurité pour une vulnérabilité de haute gravité qui peut permettre à un attaquant distant authentifié d'exécuter du code arbitraire avec des privilèges élevés.

La faille référencée CVE-2021-22908 affecte les versions 9.0Rx et 9.1Rx de Pulse Connect Secure. Dans un rapport détaillant la vulnérabilité, le CERT Coordination Center a déclaré qu'il s'agit d'une vulnérabilité de dépassement de tampon dans le code lié à Samba.

Il est recommandé aux clients Pulse Secure de mettre à niveau vers la version 9.1R.11.5 du serveur PCS dès qu'elle sera disponible. Dans l'intervalle, Ivanti a publié un fichier de solution de contournement ('Workaround-2105.xml') qui peut être importé pour désactiver la fonctionnalité Windows File Share Browser en ajoutant les points de terminaison d'URL vulnérables à une liste de blocage et ainsi activer les atténuations nécessaires pour se protéger contre cette vulnérabilité .

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

Vmware

Vulnérabilité critique dans VMware

25 mai 2021

VMware a émis un avis indiquant que les machines vCenter utilisant des configurations par défaut avaient un bug qui permet l'exécution de code malveillant lorsque les machines sont accessibles sur un port exposé à Internet.

« Un acteur malveillant disposant d'un accès réseau au port 443 peut exploiter la faille référencée CVE-2021-21985 pour exécuter des commandes avec des privilèges élevés sur le système d'exploitation sous-jacent qui héberge vCenter Server». Vmware a publié une mise à jour et des solutions de contournement pour le CVE-2021-21985.

Source : *https://bit.ly/34wdyeo*

Bluetooth

De nouvelles failles permettent aux attaquants de se faire passer pour des appareils légitimes

24 mai 2021

« Les appareils prenant en charge les spécifications Bluetooth Core et Mesh sont vulnérables aux attaques par usurpation d'identité et à la divulgation d'AuthValue qui pourraient permettre à un attaquant d'usurper l'identité d'un appareil légitime pendant l'appariement », a déclaré le Centre de coordination Carnegie Mellon CERT.

Les deux spécifications Bluetooth définissent la norme qui permet la communication de type plusieurs-à-plusieurs sur la technologie sans fil à courte portée pour faciliter le transfert de données entre les appareils dans un réseau ad-hoc.

Six failles référencées CVE-2020-26555 , CVE-2020-26558, CVE-2020-26556, CVE-2020-26557, CVE-2020-26559 , CVE-2020-26560 ont été découvertes dans les versions 1.0 et 1.0.1 de la spécification de profil de maillage Bluetooth. Le projet Android Open Source (AOSP), Cisco, Cradlepoint, Intel, Microchip Technology et Red Hat font partie des fournisseurs identifiés avec des produits concernés par ces failles de sécurité. AOSP, Cisco et Microchip Technology ont déclaré qu'ils travaillaient actuellement pour atténuer les problèmes. Le Bluetooth Special Interest Group (SIG), l'organisation qui supervise le développement des normes Bluetooth, a également publié des avis de sécurité pour chacune des six failles.

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

Apple

Une vulnérabilité dans les puces Apple M1, baptisée M1RACLES, qui ne peut pas être corrigée

28 mai 2021

Un expert en sécurité a découvert une vulnérabilité dans les nouvelles puces Apple M1, référencées CVE-2021-30747, baptisée M1RACLES.

L'expert a souligné que la gravité de la vulnérabilité est très faible et ne pose pas de risque de sécurité majeur car il existe d'autres canaux secondaires pour la fuite de données.

La vulnérabilité M1RACLES permet à deux applications exécutées sur le même appareil d'échanger des données via un canal secret au niveau du processeur, sans utiliser de mémoire, de sockets, de fichiers ou toute autre fonctionnalité normale du système d'exploitation

L'expert a expliqué qu'il craignait uniquement une éventuelle exploitation du bug par des agences de publicité frauduleuses, qui pourraient abuser d'une application déjà installée sur un appareil pour le suivi inter-applications.

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

Apple corrige des failles de sécurité dangereuses, dont une en exploitation active

25 mai 2021

Une vulnérabilité zero-day (CVE-2021-30713) qui permettrait au malware XCSSET de prendre furtivement des captures d'écran du bureau de la victime a été corrigée par Apple sur macOS 11.4.

Découvert en août 2021 par les chercheurs de Trend Micro, XCSSET est en fait un logiciel espion de type cheval de Troie qui peut récupérer les données utilisateur de Safari et d'autres navigateurs installés, lire les cookies, injecter des backdoors JavaScript sur des sites Web, récupérer des informations à partir de diverses applications (Evernote, Telegram, WeChat, etc.), faire des captures d'écran de l'utilisateur, etc.

La mise à jour du système d'exploitation apporte de nombreux correctifs de sécurité dont celle de la vulnérabilité susmentionnée. Les utilisateurs sont invités à mettre en œuvre les mises à jour dès que possible.

Source : *https://bit.ly/34zEkSU*

Actualité

Les réseaux d'entreprise sont vulnérables à des failles vieilles de 20 ans

27 mai 2021

Alors que l'industrie se concentre sur les attaques exotiques - telle que SolarWinds- le risque réel pour les entreprises provient d'exploits plus anciens, certains datant de 20 ans.

Des recherches ont montré que les attaquants recherchaient souvent des systèmes en fin de vie et non pris en charge. Les vulnérabilités et les CVE identifiées étaient des exploits ciblant des logiciels, à savoir vSphere, Oracle WebLogic et Big-IP, ainsi que des routeurs présentant des vulnérabilités d'administration à distance.

Les correctifs peuvent résoudre la majorité des problèmes. Cependant, les entreprises estiment qu'il est difficile de rester au fait des correctifs et que les systèmes de sécurité hérités sont souvent insuffisants pour arrêter les menaces. De plus, les acteurs de la menace modifient constamment leurs signatures et leurs caractéristiques pour éviter d'être détectés.

Si elles ne sont pas correctement sécurisées, ces applications peuvent être ciblées par des attaquants engendrant des conséquences désastreuses, comme l'ont montré les récentes attaques contre le système d'approvisionnement en eau de Floride, Molson Coors et Colonial Pipeline […].

Les réseaux d'entreprise continuent également d'être alimentés par des applications grand public, la plus populaire étant TikTok qui avait des millions de flux de plus que Google Mail, LinkedIn ou Spotify […].

Source *: https://bit.ly/3wIfXP1*

Des chercheurs mettent en garde contre la propagation des rootkits Linux par Facefish.

28 mai 2021

Des chercheurs en cybersécurité ont dévoilé un nouveau programme de porte dérobée capable de voler les identifiants de connexion utilisateur, des informations sur les appareils et d'exécuter des commandes arbitraires sur les systèmes Linux.

Le logiciel malveillant a été surnommé «Facefish » par l'équipe Qihoo 360 NETLAB en raison de ses capacités à fournir différents rootkits à différents moments et de l'utilisation du chiffrement Blowfish pour crypter les communications vers le serveur contrôlé par l'attaquant […].

L'étude de NETLAB s'appuie sur une analyse précédente publiée par Juniper Networks le 26 avril, qui documentait une chaîne d'attaque ciblant Control Web Panel (CWP, anciennement CentOS Web Panel) pour injecter un implant SSH avec des capacités d'exfiltration de données.

Les résultats de NETLAB proviennent d'une analyse d'un exemple de fichier ELF détecté en février 2021. D'autres indicateurs de compromission associés au malware sont accessibles ici .

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

Les publicités ciblées d'AnyDesk sur Google ont servi d'application armée

27 mai 2021

Une fausse version de la populaire application de bureau à distance AnyDesk, diffusée via des publicités apparaissant dans les résultats de recherche Google, a servi une version piégée du programme. La campagne a même battu la propre campagne publicitaire d'AnyDesk sur Google - se classant plus haut dans ses résultats payants.

Selon un rapport publié par crowdstrike, la campagne, active depuis le 22 avril, est remarquable parce que les criminels derrière la publicité malveillante ont réussi à éviter le contrôle de filtrage anti-malvertising de Google. En conséquence, les chercheurs de Crowdstrike estiment que 40% de ceux qui ont cliqué sur l'annonce ont vraisemblablement installé le malware. 20% de ces installations comprenaient des «activités follow-on hands-on-keyboard» par des criminels du système de la victime.

Crowdstrike a informé les clients concernés et a alerté Google de l'abus publicitaire.

« Il semble que Google ait rapidement pris les mesures appropriées, car au moment de la publication de ce blog, l'annonce n'était plus diffusée », note le rapport.

Source *: https://bit.ly/3i0kjwY*

Des milliers d'extensions Chrome altèrent les en-têtes de sécurité

25 mai 2021

Des milliers d'extensions Google Chrome disponibles sur le Chrome Web Store officiel falsifient les en-têtes de sécurité des sites Web populaires, exposant les utilisateurs à un large éventail d'attaques Web.

Au niveau technique, un en-tête de sécurité est une réponse HTTP envoyée par le serveur à une application cliente, telle qu'un navigateur [….

Les en-têtes de sécurité sont un type de réponse HTTP qui a été créée au fil des ans par des groupes de normes Internet pour permettre aux administrateurs de sites Web d'activer et de personnaliser les fonctionnalités de sécurité dans le navigateur de l'utilisateur ou d'autres applications clientes.

Dans un article présenté à l'atelier MADWeb lors de la conférence sur la sécurité NDSS 2021, des chercheurs du CISPA

Helmholtz Center for Information Security ont déclaré avoir tenté d'évaluer le nombre d'extensions Chrome altérant les en-têtes de sécurité.

Leur travail a révélé que 2485 extensions interceptaient et modifiaient au moins un en-tête de sécurité utilisé par les 100 sites Web les plus populaires d'aujourd'hui (liste Tranco).

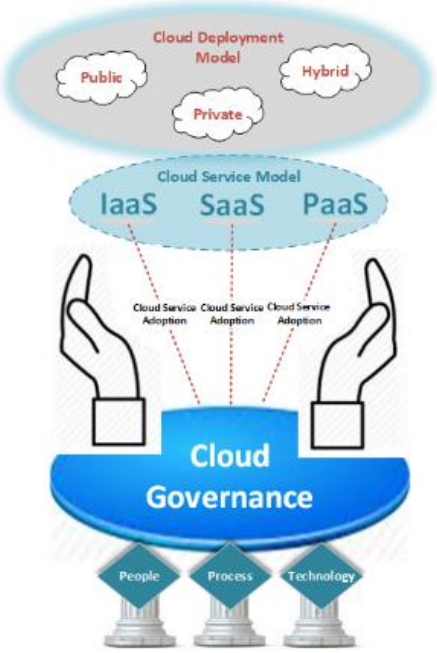
L'étude ne s'est pas concentrée sur tous les en-têtes de sécurité, mais uniquement sur les quatre plus courants, tels que: Content-Security Policy (CSP), HTTP Strict-Transport-Security (HSTS), X-Frame-Options et X- Options de type de contenu .

Des détails supplémentaires peuvent être trouvés dans un article de recherche intitulé « First, Do No Harm : Studying the manipulation of security headers in browser extensions», disponible ici [PDF].

Source : *https://bit.ly/3yP1OS3*

Cloud … soyons prêts !

Gouvernance du Cloud : Importance et éléments de base



81 % des décideurs mondiaux du cloud affirment que la sécurité est le principal défi à relever dans ce domaine. Les entreprises se lancent souvent dans des initiatives cloud sans être correctement préparées aux complexités auxquelles elles seront confrontées. Le taux de réussite des projets cloud est considérablement impacté si les processus de gouvernance n'abordent pas directement les caractéristiques du Cloud.

Les entreprises devraient commencer par établir des principes de gouvernance du Cloud computing. L'Open Group a défini 5 principes de gouvernance du Cloud Computing qui doivent être adoptés et appliqués tout au long du cycle de vie du Cloud :

1. **Conformité aux politiques et aux normes** - Les normes du Cloud doivent être ouvertes, cohérentes et complémentaires aux normes en vigueur dans l'industrie et adoptées par l'entreprise.
2. **Les objectifs commerciaux doivent guider la stratégie Cloud** - La stratégie cloud d'entreprise doit faire partie intégrante de la stratégie commerciale et informatique globale, motivée à la fois par les objectifs « métiers de l'entreprise » et « métier de l'informatique » pour l'entreprise.
3. **Contrats de collaboration entre les citoyens de l'écosystème Cloud -** un ensemble clair de règles et d'accords définissant l'interaction entre les parties prenantes est essentielle pour permettre leur coexistence saine au sein de l'écosystème Cloud.
4. **Adhésion aux processus de gestion du changement** - Le changement doit être exercé et appliqué de manière cohérente et normalisée à travers tous les composants de l'écosystème Cloud de l'entreprise.
5. **Application des processus de vitalité pour parvenir à une amélioration continue** - Les processus de gouvernance de cloud doivent surveiller dynamiquement les événements qui déclenchent des améliorations continues.

Les environnements cloud peuvent être difficile à gérer sans une gouvernance cloud efficace, car ils sont souvent indisciplinés et imprévisibles. Il est donc très important de disposer de solides contrôles de gouvernance et de gestion du cloud, parfaitement alignés sur les buts et objectifs de l'organisation, soutenus à tous les niveaux du parcours du Cloud et synchronisés avec les cadres, les méthodologies et les normes de l'entreprise.

Source : *https://bit.ly/2ROBGX2*

Bon à savoir !

Les risques d'utilisation des outils d'accès à distance TeamViewer, AnyDesk, VNC…!

Les outils d'accès à distance largement utilisés aujourd'hui incluent Microsoft Remote Desktop, TeamViewer, Telnet, Citrix XenDesktop et VNC… permettent à un utilisateur de contrôler le bureau d'un autre poste.

Tous les types de logiciels, y compris les outils d'accès à distance, peuvent présenter des vulnérabilités qui pourraient être exploitées par des personnes malveillantes. De telles vulnérabilités sont encore plus facile à exploiter quand le poste est déjà ouvert sur internet et leur impact n'est que plus néfaste.

L'un des plus grands problèmes de la cyber sécurité provient de l'utilisation naïve, non protégée et non cadrée de tout type d'outils augmentant par conséquence la surface d'attaque pour les personnes malveillantes.

De par les risques importants induits par l'utilisation des outils d'accès à distance ou les bureaux distants, il est important de respecter quelques règles de sécurité afin de minimiser ces risques :

- Autoriser l'accès basé sur la justification pour sélectionner les utilisateurs qui en ont besoin
- L'outil ne doit pas être exécuté au démarrage de l'ordinateur
- Limiter son utilisation au besoin et le désactiver le cas échéant
- Utiliser un mot de passe fort et le changer régulièrement
- Activer l'authentification multifactorielle quand c'est possible
- Ne pas utiliser une version crackée
- La solution de bureau à distance utilisée doit offrir des fonctionnalités de sécurité essentielles.

Evènements

Evènements du mois

SOMMET VIRTUEL SUR LA CYBERSÉCURITÉ : MOYEN-ORIENT

19-20 mai 2021, Online

https://bit.ly/3uEgHDj

La région du Moyen-Orient a connu une numérisation rapide en passant au télétravail et en adoptant une approche accélérée d'une stratégie « cloud-first ». Cela a permis l'expansion de l'innovation et l'ouverture de nouvelles passerelles pour les cyberattaques et autres perturbations opérationnelles.

Les experts confirment que l'année 2021 sera marquée par des risques tiers, une augmentation des cas d'informatique parallèle, une croissance des vulnérabilités dans les réseaux de communication numérique et les chaînes d'approvisionnement, car tous les secteurs investissent dans les technologies de l'information et de la communication, avec une attention minimale aux exigences de cybersécurité.

Ce sommet virtuel a permis aux auditeurs d'obtenir des informations d'experts de la part de praticiens, de chercheurs et de fournisseurs sur la manière dont les RSSI devraient s'attaquer aux risques découlant de ces tendances, s'adapter et aller de l'avant pour bâtir une cyber-entreprise résiliente, même si le terrain continue de changer.

Evènements à venir

Webnair : Security by Design dans le développement de logiciels

16 juin 2021, Online

https://bit.ly/3vC0W11

Pour être en mesure de fournir un logiciel conforme aux standards en matière de sécurité, il faut que des pratiques de codage sécurisées y soit intégrées dès sa conception. Dans cet exposé, le speaker présentera comment les principes et objectifs de sécurité largement reconnus dans l'industrie peuvent être inculqués dans le cycle de vie du développement logiciel en tant qu'éléments concrets et exploitables. Cela rend le travail lié à la sécurité explicite, mesurable et aide à équilibrer les coûts et les avantages impliqués.

Reference	ANPT-2021-BV-05
Titre	Bulletin de veille N°05
Date de version	31 Mai 2021
Contact	ssi@anpt.dz