BULLETIN DE VEILLE N°06

ANPT-2022-BV-06

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

Juin 2022

Alertes de sécurité

Microsoft

Microsoft corrige 55 vulnérabilités dans le Patch Tuesday de juin 2022

14 Juin 2022

Microsoft a corrigé un total de 55 vulnérabilités à travers son Patch Tuesday de juin 2022, dont une est de type 'zero-day' connue sous le nom de « Follina ».

La mise à jour porte des correctifs pour 03 failles considérées comme étant critiques car elles permettent l'exécution de code à distance, et le reste est classé comme important. Ceci n'inclut pas les 5 mises à jour Microsoft Edge Chromium qui ont été publiées précédemment ce mois.

Le nombre de bogues dans chaque catégorie de vulnérabilité est indiqué comme suit :

- 12 vulnérabilités d'élévation de privilège ;
- 1 vulnérabilité liée au contournement d'une fonction de sécurité ;
- 27 vulnérabilités d'exécution de code à distance ;
- 11 vulnérabilités liées à la divulgation d'informations ;
- 3 vulnérabilités de déni de service ;
- 1 vulnérabilité liée à l'usurpation d'identité.

Il est recommandé de mettre à jour les systèmes affectés ou d'appliquer les mesures d'atténuation afin d'éviter toute menace possible.

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

Adobe

46 failles de sécurité corrigées par Adobe dans le cadre du Patch Tuesday

14 Juin 2022

Dans le cadre de son Patch Tuesday de juin, Adobe a publié des correctifs pour au moins 46 vulnérabilités de sécurité concernant une large gamme de produits logiciels destinés aux entreprises. Elles peuvent exposer les utilisateurs de Windows et de macOS à des attaques malveillantes.

Les failles les plus graves affectent les produits suivant :

- Adobe Animate versions 22.0.5 et antérieures : La mise à jour résout un bogue critique qui pourrait conduire à une exécution de code arbitraire dans le contexte de l'utilisateur actuel.
- Adobe Bridge versions 12.0.1 et antérieures : La mise à jour apporte des correctifs pour 12 vulnérabilités criques et importantes qui pourraient conduire à une exécution de code arbitraire, une écriture arbitraire du système de fichiers et une fuite de mémoire.
- Adobe Illustrator 2021 et 2022 : La mise à jour résout 17 failles critiques, importantes et modérées pouvant entraîner une exécution de code arbitraire et une fuite de mémoire.
- Adobe InCopy : La mise à jour corrige 8 problèmes critiques. Une exploitation réussie pourrait conduire à une exécution de code arbitraire.
- Adobe InDesign : La mise à jour corrige 7 faiblesses critiques. Elles ont le même impact que celles d'Adobe InCopy.

Adobe invite ses clients à appliquer les mises à jour ou les mesures d'atténuation pour empêcher les attaquants à nuire la sécurité de leurs entreprises.

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

Parse Server

Un sévère bogue du serveur Parse affecte Apple Game Center

22 Juin 2022

Une vulnérabilité a été découverte dans le logiciel Parse Server qui conduit à un contournement d'authentification affectant Apple Game Center.

Parse Server est un logiciel open source disponible sur GitHub qui fournit une fonctionnalité de notification push pour iOS, macOS, Android et tvOS.

Suivie sous le nom de CVE-2022-31083 et dotée d'un score de gravité CVSS de 8.6, la faille est décrite comme un scénario dans lequel l'adaptateur d'authentification pour le certificat de sécurité d'Apple Game Center n'est pas validé. La complexité de l'attaque est considérée comme faible et aucun privilège n'est requis.

"En conséquence, l'authentification pourrait potentiellement être contournée en rendant un faux certificat accessible via certains domaines Apple et en fournissant l'URL de ce certificat dans un objet authData", indique l'avis de sécurité publié sur GitHub.

Parse Server a corrigé le problème en publiant la version 4.10.11 et 5.2.2. Le logiciel a implémenté une nouvelle propriété rootCertificateUrl dans l'adaptateur d'authentification Apple Game Center, qui prend "la valeur de l'URL du certificat racine du certificat d'authentification Game Center d'Apple". Dans le cas où les développeurs n'ont pas défini de valeur dans le système d'authentification, la nouvelle propriété prend par défaut l'URL du certificat racine utilisé par Apple.

La meilleure méthode d'éviter les risques potentiels de cette faille est d'appliquer les derniers correctifs dès que possible sur les appareils.

Source : https://bit.ly/3uao6No

OpenSSL

OpenSSL publiera un correctif de sécurité pour la vulnérabilité critique

27 Juin 2022

Une vulnérabilité a été découverte dans la dernière version d'OpenSSL qui pourrait permettre à un acteur de la menace de provoquer une corruption de mémoire à distance sur certains systèmes.

OpenSSL 3.0.4 a été récemment publié pour corriger une vulnérabilité d'injection de commande (CVE-2022-2068) qui n'a pas été entièrement corrigée par un correctif précédent (CVE-2022-1292). Mais, Selon le chercheur Guido Vranken, cette version nécessite elle-même des corrections supplémentaires pour corriger un problème dans les systèmes x64 avec le jeu d'instructions AVX-512 qui pourrait provoquer une corruption de mémoire à distance.

Le bogue a été corrigé après avoir été signalé, mais la version 3.0.5 d'OpenSSL n'a pas encore été publiée et Tomáš Mráz de la Fondation OpenSSL a déclaré "Je ne pense pas qu'il s'agisse d'une vulnérabilité de sécurité, Il s'agit simplement d'un bogue sérieux rendant la version 3.0.4 inutilisable sur les machines capables d'utiliser AVX-512".

Alex Gaynor, ingénieur en résilience logicielle au sein de l'US Digital Service, soutient toutefois le contraire.

"Je ne suis pas sûr de comprendre comment il ne s'agit pas d'une vulnérabilité de sécurité", a répondu Gaynor. "C'est un dépassement de tampon de tas qui peut être déclenché par des choses comme les signatures RSA, ce qui peut facilement se produire dans des contextes distants (par exemple, une poignée de main TLS)". Comme il insiste pour qu'un correctif soit publié rapidement.

Source : *https://bit.ly/3noR4oX*

Citrix

Citrix corrige une faille critique qui réinitialise les mots de passe des administrateurs

15 Juin 2022

Citrix a mis en garde contre une vulnérabilité critique dans Citrix Application Delivery Management (ADM) une solution de gestion centralisée, la faille pourrait permettre à un attaquant non authentifié de se connecter en tant qu'administrateur.

Repéré sous le nom de CVE-2022-27511, le bogue est décrit comme un problème de contrôle d'accès inapproprié qui pourrait permettre à un attaquant distant non authentifié de corrompre le système et de déclencher une réinitialisation du mot de passe de l'administrateur.

Une deuxième faille a été résolue (CVE-2022-27512), qui est un problème lié à un contrôle inapproprié des ressources, il pourrait entraîner une interruption temporaire du service de licence ADM, empêchant ainsi Citrix ADM d'émettre de nouvelles licences ou de renouveler les licences existantes.

Les clients sont invités à effectuer une mise à jour vers Citrix ADM 13.1-21.53 ou les versions ultérieures de 13.1, ou Citrix ADM 13.0-85.19 ou les versions ultérieures de 13.0, qui contiennent les correctifs nécessaires. Le serveur Citrix ADM et tous les agents Citrix ADM associés doivent être mis à jour.

Source : *https://bit.ly/3nq38X7*

Cisco

Cisco a publié des correctifs pour une vulnérabilité critique qui affecte ses produits Email Security Appliance (ESA) et Secure Email and Web Manager

16 Juin 2022

Cisco a publié des correctifs pour une vulnérabilité critique qui affecte ses produits Email Security Appliance (ESA) et Secure Email and Web Manager.

Identifiée sous le nom de CVE-2022-20798 avec un score CVSS de 9.8, la faille peut être exploitée à distance pour contourner l'authentification et se connecter à l'interface de gestion Web des appareils concernés.

Selon Cisco, la faille est due à des vérifications d'authentification incorrectes quand un appareil affecté utilise le protocole LDAP (Lightweight Directory Access Protocol) pour l'authentification externe. Un attaquant pourrait exploiter cette vulnérabilité en saisissant une entrée spécifique sur la page de connexion de l'appareil exécutant une version vulnérable de logiciel AsyncOS.

Une deuxième vulnérabilité (connue sous le nom CVE-2022-20664) a été corrigée par Cisco, le problème existe parce que les données d'entrée ne sont pas correctement vérifiées lors de l'interrogation du serveur d'authentification externe.

Il est recommandé d'appliquer les correctifs nécessaires afin d'atténuer les risques potentiels.

Source : *https://bit.ly/3QVjF2M*

Actualité

Les dispositifs Bluetooth peuvent être utilisés pour localiser les téléphones portables !

En utilisant les signaux Bluetooth générés par les smartphones, des chercheurs en sécurité de l'université de Californie à San Diego ont mis au point une méthode permettant d'identifier et de suivre les personnes via leurs smartphones.

Au cours des recherches de l'équipe, ils ont découvert que les signaux Bluetooth, qui sont envoyés en permanence par les téléphones, ont une empreinte digitale unique qui peut être identifiée.

En outre, ils se sont également inquiétés du fait que les pirates informatiques pourraient exploiter cette technologie afin de localiser une cible. Grâce à cette nouvelle technique, les mesures de protection actuelles contre le harcèlement téléphonique pourraient être facilement contournées.

Certaines recherches menées auparavant ont montré que l'empreinte digitale sans fil est présente dans les technologies sans fil telles que le WiFi. Ce type de suivi, comme l'a souligné l'équipe de l'université de Californie à San Diego, peut également être réalisé à l'aide de Bluetooth avec une précision parfaite.

Le Bluetooth pose de plus en plus de problèmes dans le monde moderne, car il s'agit non seulement d'un signal sans fil qui émet une multitude de signaux, mais aussi d'un signal continu qui est émis en permanence par les appareils intelligents.

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

Un malware contrôlant des milliers de sites du réseau Parrot TDS

Le système de direction du trafic (TDS) Parrot qui a été révélé au début de l'année a eu un impact plus important qu'on ne le pensait, selon une nouvelle recherche.

Parrot TDS a été documenté en avril 2022 par la société Avast, qui a indiqué que le script PHP avait pris au piège des serveurs Web hébergeant plus de 16 500 sites Web pour servir de passerelle à d'autres campagnes d'attaque.

Il permet d'ajouter un élément de code malveillant à tous les fichiers JavaScript sur les serveurs Web compromis hébergeant des systèmes de gestion de contenu (CMS) tels que WordPress, qui seraient à leur tour violés en profitant d'identifiants de connexion faibles et de plugins vulnérables.

L'objectif du code JavaScript est de lancer la deuxième phase de l'attaque, qui consiste à exécuter un script PHP déjà déployé sur le serveur et conçu pour recueillir des informations sur un visiteur du site (adresse IP, référent, navigateur, etc.) et transmettre ces détails à un serveur distant.

La troisième couche de l'attaque arrive sous la forme d'un code JavaScript du serveur, qui agit comme un système de direction du trafic pour décider de la charge utile exacte à délivrer pour un utilisateur spécifique en fonction des informations partagées à l'étape précédente.

"Une fois que le TDS a vérifié l'éligibilité d'un visiteur spécifique du site, le script NDSX charge la charge utile finale à partir d'un site Web tiers", a déclaré le chercher Denis Sinegubko. Le malware de troisième étape le plus couramment utilisé est un téléchargeur JavaScript nommé FakeUpdates (alias SocGholish).

Rien qu'en 2021, Sucuri a déclaré avoir supprimé Parrot TDS de près de 20 millions de fichiers JavaScript trouvés sur des sites infectés. Au cours des cinq premiers mois de 2022, plus de 2 900 fichiers PHP et 1,64 million de fichiers JavaScript contenant le malware ont été observés.

"La campagne de logiciels malveillants NDSW est extrêmement réussie car elle utilise une boîte à outils d'exploitation polyvalente qui ajoute constamment de nouvelles vulnérabilités divulguées et 0-day", explique Sinegubko.

"Une fois que le mauvais acteur a obtenu un accès non autorisé à l'environnement, il ajoute diverses portes dérobées et des utilisateurs d'administration CMS pour maintenir l'accès au site Web compromis longtemps après la fermeture de la vulnérabilité originale."

***Source :** https://bit.ly/3QTvJS7*

Des campagnes de phishing par messagerie vocale

Les acteurs de menace ont lancé une nouvelle campagne de phishing par messagerie vocale afin de voler les identifiants Outlook et les identifiants de connexion à Microsoft Office 365.

L'objectif de cette campagne en cours est d'inciter les victimes à ouvrir une pièce jointe HTML malveillante via de fausses notifications de messagerie vocale utilisées par les pirates pour attirer leurs victimes.

L'e-mail utilisé par les acteurs de la menace contient une pièce jointe qui semble être un clip sonore en raison de l'utilisation d'un caractère de note de musique dans la convention de dénomination.

Un site de phishing est en fait caché dans le code JavaScript obscurci contenu dans le fichier. Afin de donner l'impression que le site est un sous-domaine légitime de l'organisation ciblée, le format de l'URL suit une méthode d'assemblage basée sur le domaine de l'entreprise ciblée.

Au cours de cette redirection, la victime est dirigée vers une page de vérification CAPTCHA. Cette vérification a pour but d'éviter que l'activité suspecte ne soit repérée par les outils anti-phishing et de donner à la victime un faux sentiment de légitimité.

L'utilisateur est redirigé ensuite vers une page de phishing qui semble authentique et qui lui vole ses informations d'identification Microsoft Office 365.

Par conséquent, les utilisateurs doivent toujours s'assurer qu'ils se trouvent sur le bon portail de connexion avant de remplir et d'envoyer leur nom d'utilisateur et leur mot de passe.

Source : *https://bit.ly/3np81cq*

Google alerte contre le spyware Hermit

Google met en garde les utilisateurs d'appareils mobiles Android et iOS contre la diffusion massive d'une variante du spyware Hermit.

Après avoir analysé 16 de ses 25 modules connus, les chercheurs en cybersécurité de Lookout ont expliqué que le logiciel malveillant s'enracine dans les appareils infectés pour enregistrer des contenus audios, pour rediriger ou effectuer des appels téléphoniques ou encore pour voler des données privées.

Selon Lookout, les souches du virus ne se trouvent pas dans les dépôts d'applications officiels de Google ou d'Apple, mais dans des applications chargées de logiciels espions téléchargées à partir d'hôtes tiers.

La circulation de Hermit ne fait que mettre en lumière un problème plus large : l'industrie florissante des logiciels espions et de la surveillance numérique.

Selon les équipes de Google, plus de 30 fournisseurs proposent actuellement des exploits ou des logiciels espions à des entités soutenues par des gouvernements.

Pour Charley Snyder, résponsable de la politique de cybersécurité chez Google, bien que leur utilisation puisse être légale, « on constate souvent qu'ils sont utilisés par des gouvernements à des fins contraires aux valeurs démocratiques : cibler des dissidents, des journalistes, des défenseurs des droits humains et des politiciens ».

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

La NSA invitent les administrateurs système à utiliser PowerShell pour détecter les activités malveillantes

La National Security Agency (NSA) a publié un avis dans lequel elle recommande aux administrateurs système d'utiliser PowerShell pour gérer les systèmes puisque les cyberattaques s'appuient fortement sur ce dernier, principalement dans la phase de post-exploitation, afin d'atteindre leurs objectifs. L'outil de configuration et d'automatisation de Microsoft peut également être utile aux défenseurs grâce à ses fonctions de sécurité intégrées.

PowerShell est un outil essentiel pour assurer la sécurité du système d'exploitation Windows, d'autant plus qu'il n'y a plus de limitations dans les nouvelles versions de PowerShell.

La configuration et la maintenance correctes de PowerShell peuvent en faire un outil fiable s'il est géré correctement pour la maintenance du système, le Forensics, l'automatisation et les tâches de sécurité.

Il est essentiel de gérer et d'adopter correctement PowerShell, ainsi que ses capacités d'administration et ses fonctions de sécurité.

Source : *https://bit.ly/3y02AMv*

Des campagnes actives de diffusion du ransomware HelloXD qui installe une porte dérobée sur les systèmes Windows et Linux ciblés

Les systèmes Windows et Linux sont la cible d'une variante de ransomware appelée HelloXD, les infections impliquant le déploiement d'une porte dérobée pour faciliter l'accès à distance persistant aux hôtes infectés.

"Contrairement à d'autres groupes de ransomware, cette famille de ransomware ne dispose pas d'un site de fuite actif ; elle préfère orienter la victime vers des négociations par le biais du chat Tox et d'instances de messagerie en oignon", ont déclaré Daniel Bunce et Doel Santos, chercheurs en sécurité de l'unité 42 de Palo Alto Networks, dans un article.

HelloXD a fait surface dans la nature le 30 novembre 2021, et est basé sur une fuite de code de Babuk, qui a été publié sur un forum de cybercriminalité en langue russe en septembre 2021.

Cette famille de ransomwares ne fait pas exception à la règle, car les opérateurs suivent l'approche éprouvée de la double extorsion pour exiger des paiements en crypto-monnaies en exfiltrant les données sensibles d'une victime en plus de les crypter et de menacer de rendre ces informations publiques.

Les fonctionnalités de MicroBackdoor permettent à un attaquant de parcourir le système de fichiers, de télécharger des fichiers, d'exécuter des commandes et d'effacer les preuves de sa présence sur les machines compromises. On soupçonne que le déploiement de la porte dérobée est effectué pour "surveiller la progression du ransomware".

Ces conclusions interviennent alors qu'une nouvelle étude d'IBM X-Force a révélé que la durée moyenne d'une attaque de ransomware d'entreprise - c'est-à-dire le temps entre l'accès initial et le déploiement du ransomware - a diminué de 94,34 % entre 2019 et 2021, passant de plus de deux mois à seulement 3,85 jours.

"L'achat d'accès peut réduire considérablement le temps nécessaire aux opérateurs de ransomware pour mener une attaque en permettant la reconnaissance des systèmes et l'identification des données clés plus tôt et avec plus de facilité", a déclaré Intel 471 dans un rapport soulignant les relations de travail étroites entre les IAB et les équipes de ransomware.

"En outre, à mesure que les relations se renforcent, les groupes de ransomware peuvent identifier une victime qu'ils souhaitent cibler et le marchand d'accès pourrait leur fournir l'accès une fois qu'il est disponible."

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

Bon à savoir !

Les nouvelles tendances du physhing

En plus d'augmenter en volume, les attaques de phishing ont pris des tournures inattendues cette année. Selon le rapport trimestriel Threat Trends & Intelligence Report, les attaques de phishing sont diffusées via différentes plateformes en ligne.

Au premier trimestre 2022, près de 52 % des sites de phishing ont été mis en scène via des sites compromis.

Environ 66 % de tous les sites de phishing ont été mis en scène sur quatre domaines génériques de premier niveau, soit une augmentation de 9,1 % par rapport au quatrième trimestre 2021.

Si l'on constate une légère augmentation des attaques traditionnelles de phishing par e-mail, les autres tendances sont les escroqueries par usurpation d'identité sur les médias sociaux, les menaces du dark web, les attaques hybrides de vishing et les attaques BEC.

Les médias sociaux sont devenus un canal favorable pour les attaquants puisque les attaques ont augmenté de 105 % depuis l'année dernière à la même époque. Les cyberattaquants disposent de multiples vecteurs pour abuser de leurs victimes, car les organisations utilisent diverses plateformes pour mener leurs opérations et communiquer.

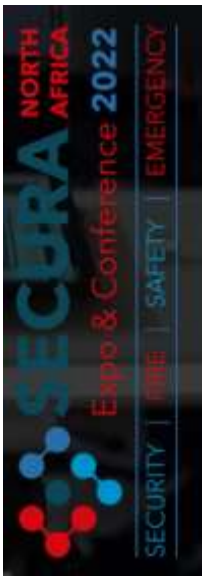
Les statistiques et incidents montrent que la sécurisation du périmètre du réseau ne suffit pas pour protéger les entreprises contre les attaques de phishing. Pour avoir une meilleure visibilité sur le paysage des menaces, les entreprises doivent surveiller les menaces de manière proactive et recueillir des renseignements sur les menaces.

Source : *https://bit.ly/3Np1nnC*

Evènements

Evènement du mois

Secura North Africa



28-30 Juin 2022

Palais des Expositions d'Alger

https://bit.ly/3I8ClIw

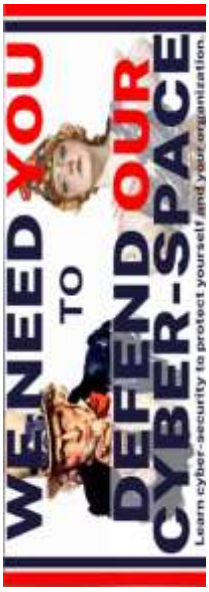
Le plus grand événement de sûreté et de sécurité en Afrique du Nord.

Cet événement a pour objectif de rassembler au même endroit pendant trois jours tous les acteurs et professionnels de ces six domaines différents :

- Santé et Sécurité au travail ;
- Sécurité industrielle et intérieure ;
- Sécurité électronique. ;
- Gestion des urgences ;
- Protection physique ;
- Détection, prévention et lutte contre les incendies.

Evènement à venir

CYBER CLINIC: Pragmatic Cyber-Security for Start-ups and SMBs



01 Juillet 2022

Online

https://bit.ly/3OM70NO

Cet évènement a pour objectif d'améliorer les pratiques de cybersécurité qu'une start-up ou une PME peut utiliser pour améliorer ses cyberdéfenses. Il se concentre sur une cyber-sécurité basé sur les conditions ou les circonstances du monde réel, en considérant ce qui peut être fait de manière réaliste, par opposition à la meilleure ligne de conduite théorique.

La session va couvrir les points suivants :

- Une stratégie pragmatique de cybersécurité pour les PME.
- Les conseils officiels du gouvernement américain en matière de cybersécurité et les programmes de soutien aux PME.
- La technologie de cybersécurité dont vous disposez peut-être déjà et comment l'utiliser efficacement.
- Vous apprendrez à mieux vous défendre et à mieux défendre votre organisation.

Référence	ANPT-2022-BV-06
Titre	Bulletin de veille N°06
Date de version	30 Juin 2022
Contact	ssi@anpt.dz