BULLETIN DE VEILLE N°08

ANPT-2021-BV-08

« True Cyber Security is preparing for what's next, not what was last.»
- Neil Rerup-

Août 2021

Alertes de sécurité

Microsoft

Patch Tuesday du mois d'aout

10 Août 2021

Dans le Patch Tuesday de ce mois, Août 2021, Microsoft a corrigé 44 failles, dont treize (13) sont des exécutions de code à distance, huit (08) sont des divulgations d'informations, deux (02) sont des dénis de service et quatre (04) sont des vulnérabilités d'usurpation d'identité.

Parmi les produits affectés par ces mises à jour, nous trouvons : ASP .NET, Azure, Microsoft Dynamics, Windows MSHTML Platform, Microsoft Graphics Component, Microsoft Office.

Ce patch comprend les correctifs de trois vulnérabilités de type Zero-Day : PrintNightmare (CVE-2021-36936), PetitPotam (CVE-2021-36942) et une vulnérabilité d'élévation de privilèges, activement exploitée (CVE-2021-36948).

Les vulnérabilités résolues avec leurs descriptions ainsi que les systèmes qu'elles affectent sont listées dans ce rapport.

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

Adobe

Des vulnérabilités d'exécution de code dans les logiciels Adobe

17 Août 2021

Adobe a émis un avertissement concernant deux failles de sécurité majeures affectant son logiciel Photoshop avec des scores CVSS de 7,8. Ces failles, classées critiques, exposent les utilisateurs de Windows et de MacOS à des attaques par exécution de code.

Les mises à jour, disponibles pour Photoshop 2020 et Photoshop 2021, sont diffusées via le mécanisme de mise à jour automatique du logiciel.

Adobe a également diffusé un correctif pour couvrir plusieurs failles d'exécution de code dans le kit SDK Adobe XMP Toolkit.

Source: *https://bit.ly/3B5qrdE*

Red Hat

Multiples vulnérabilités dans le noyau Linux de Red Hat

19 Août 2021

Des mises à jour pour le noyau Red Hat Entreprise Linux 8.1 ont été publiées afin de corriger des vulnérabilités permettant de provoquer un déni de service et une élévation de privilèges.

Les vulnérabilités en question sont les suivantes :

CVE-2021-22543 : Cette faille permet aux utilisateurs qui peuvent démarrer et contrôler une VM, de lire/écrire des pages de mémoire aléatoires, ce qui peut entraîner une élévation locale des privilèges.

CVE-2021-22555 : Cette faille permet à un utilisateur local d'obtenir des privilèges ou de provoquer un DoS.

CVE-2021-32399 : Cette faille permet à un attaquant disposant d'un compte local d'altérer la mémoire et de causer, éventuellement, une élévation des privilèges.

Plus de détails sur les vulnérabilités et les versions affectées sont disponible sur l'avis de sécurité de Red Hat.

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

Pulse Secure

Une mise à jour urgente pour les appliances VPN

09 Août 2021

Pulse Secure a expédié un correctif pour une vulnérabilité critique d'exécution de code à distance après authentification dans ses appliances VPN Connect Secure, et cela afin de remédier à un correctif incomplet pour une faille activement exploitée qu'elle a précédemment résolue en octobre 2020.

Référencée par CVE-2021-22937 (score CVSS : 9.1), la faille pourrait "permettre à un administrateur authentifié d'effectuer une écriture de fichier via une archive, malicieusement conçue, téléchargée dans l'interface Web de l'administrateur", selon Pulse Secure

Cette divulgation intervient quelques jours après qu'Ivanti, la société à l'origine de Pulse Secure, ait publié le 2 août un avis concernant pas moins de six vulnérabilités de sécurité, exhortant les clients à procéder rapidement à la mise à jour vers la version 9.1R12 de Pulse Connect Secure afin de se prémunir contre toute tentative d'exploitation de ces failles.

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

IBM WebSphere

De multiples vulnérabilités dans IBM Java SDK affectent le processeur WebSphere Application Server

19 Août 2021

Il existe de multiples vulnérabilités dans l'IBM SDK Java Technology Edition qui est livré avec IBM WebSphere Application Server, pouvant permettre à un attaquant de provoquer une exécution de code arbitraire à distance, un déni de service et une atteinte à la confidentialité et à l'intégrité des données.

Ces vulnérabilités affectent WebSphere Application Server 9.0 avec le SDK IBM Java version 8 antérieures à R6 FP35, WebSphere Application Server 8.5.x.x sans le dernier correctif et WebSphere Application Server Liberty avec le SDK IBM Java version 8 antérieures à R6 FP35.

Plus de détails sont listés dans le bulletin de sécurité d'IBM. Les utilisateurs de cette technologie sont invités à le consulter et à appliquer les correctifs.

Sources : *https://bit.ly/3zlaL5y*

Cisco

Des failles critiques dans les routeurs Cisco qui permettent aux attaquants d'exécuter un code arbitraire

06 Août 2021

Cisco a publié des correctifs de sécurité critiques pour résoudre les bugs des routeurs VPN pour petites entreprises. Les vulnérabilités répertoriées sous le nom de CVE-2021-1609 (score CVSS : 9,8) et CVE-2021-1610 (score CVSS : 7,2) ont été découvertes dans l'interface de gestion Web des routeurs VPN Gigabit Cisco Small Business RV340, RV340W, RV345 et RV345P Dual WAN.

Ces failles affectent les routeurs Cisco Small Business ayant une version de Firmware antérieure à la version 1.0.03.22, et permettent à un attaquant de provoquer un déni de service ou d'exécuter du code arbitraire

Cisco mentionne qu'elle a également corrigé un bug d'exécution de code à distance de haute gravité (CVE-2021-1602, score CVSS : 8.2) affectant ses routeurs VPN Small Business RV160, RV160W, RV260, RV260P et RV260W exécutant des versions de Firmware antérieures à la version 1.0.01.04.

Ce bug pourrait permettre à un attaquant distant d'exécuter des commandes arbitraires sur un dispositif affecté.

Source : *https://bit.ly/3gBCIi5*

Une vulnérabilité critique dans les anciens routeurs Small Business restera non corrigée

20 Août2021

Cisco a publié un avis de sécurité sur une vulnérabilité critique d'exécution de code (score CVSS de 9.8) affectant ses routeurs RV110W, RV130, RV130W et RV215W, mais a averti qu'il n'y a aucun plan pour publier des correctifs de sécurité.

La vulnérabilité trouvée, répertoriée CVE-2021-34730, se trouve dans le service Universal Plug-and-Play (UPnP) de Cisco Small Business, et pourrait permettre à un attaquant distant non authentifié d'exécuter du code arbitraire ou de faire redémarrer de manière inattendue un appareil vulnérable, ce qui entraînerait un déni de service (DoS).

Cisco recommande aux propriétaires des produits cités ci-dessus de désactiver UPnP sur les interfaces LAN et WAN de leurs appareils, afin d'atténuer le bug. UPnP est activé par défaut sur les interfaces LAN.

Cisco déclare qu'il n'a pas publié et ne publiera pas de mises à jour logicielles pour remédier à cette vulnérabilité, car elle affecte des produits plus anciens qui ont déjà atteint le statut de fin de vie (EOL).

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

Une faille du logiciel Cisco Firepower Device Manager permet aux attaquants d'exécuter du code à distance

05 Août 2021

Une vulnérabilité référencée CVE-2021-1518 de gravité moyenne, découverte dans l'API REST du logiciel Cisco Firepower Device Manager (FDM) On-Box, pourrait permettre à un attaquant d'exécuter du code arbitraire sur le système d'exploitation sous-jacent d'un appareil affecté.

La faille, ayant un score CVSS de 6.3, peut être exploitée par un attaquant disposant d'informations d'identification valides.

Cisco a publié des mises à jour qui corrigent cette vulnérabilité. Les utilisateurs du logiciel sont invités à les appliquer dès que possible.

Source : *https://bit.ly/3sPd4LI*

Synology

Synology touché par les vulnérabilités d'OpenSSL

26 Août 2021

Synology a révélé que des vulnérabilités OpenSSL d'exécution de code à distance et de déni de service récemment divulguées ont un impact sur certains de ses produits.

Les dispositifs affectés par les failles de sécurité suivies comme CVE-2021-3711 et CVE-2021-3712 sont DSM 7.0, DSM 6.2, DSM UC, SkyNAS, VS960HD, SRM 1.2, VPN Plus Server, et VPN Server.

Bien que l'équipe de développement d'OpenSSL ait publié OpenSSL 1.1.1l pour corriger les deux failles le 24 août, Synology dit que les versions pour les produits touchés sont soit "en cours" ou "en attente".

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

Actualité

La NSA et le CISA publient un guide sur le renforcement de Kubernetes

03 Août 2021

Kubernetes est un système open source qui vise à fournir une plateforme pour automatiser le déploiement, la mise à l'échelle et l'exécution de conteneurs d'applications sur des clusters de serveurs dans un environnement de cloud. Kubernetes est généralement ciblé pour trois raisons majeures : vol de données, vol de puissance de calcul ou déni de service.

La National Security Agency (NSA) et la Cybersecurity and Infrastructure Security Agency (CISA) ont publié un rapport technique intitulé "Kubernetes Hardening Guidance", qui détaille les menaces potentielles qui pèsent sur le système Kubernetes et fournit des conseils de configuration pour minimiser les risques.

CISA a également publié un nouveau guide de formation téléchargeable destiné à la main-d'œuvre de la cybersécurité.

Publié en août 2021, le guide "Cybersecurity Workforce Training" peut aider les professionnels de la cybersécurité de tous niveaux à rester à jour et à faire progresser leur carrière

Sources *: https://bit.ly/3DbLtsX ; https://bit.ly/3zj9SdV*

Messenger intègre des fonctions de chiffrement de bout en bout des conversations

13 Août 2021

Le chiffrement de bout en bout (E2EE) est une fonctionnalité de sécurité qui empêche des tiers d'écouter les appels et les chats entre les interlocuteurs.

Cette fonctionnalité est bien disponible pour les conversations textuelles sur le service de messagerie de Facebook depuis 2016. Facebook a déclaré le 13 août dernier avoir étendu la possibilité d'utiliser le chiffrement de bout en bout, notamment, pour les appels vocaux et vidéo sur Messenger, autrement dit étendre la protection aux appels vocaux et vidéo sur Messenger, ce qui signifie que personne d'autre, y compris Facebook theoriquement), ne peut voir ou entendre ce qui est envoyé ou dit ente les abonnés.

Source *: https://bit.ly/3zqG92k*

Black Hat USA 2021 : Les outils de sécurité présentés

05 Août 2021

Depuis l'édition 2017, la conférence Black Hat USA est devenue un lieu où la communauté de la cybersécurité annonce toutes les dernières nouvelles et où les outils de sécurité les plus récents sont publiés.

Cette année, la conférence a révélé les derniers travaux et exploits dans le domaine. Des outils développés à des fins de sécurité ont été présentés aussi. Ci-dessous quelques outils parmi les plus intéressants de la conférence de cette année :

- Phishmonger : un outil de phishing par e-mail qui permet aux testeurs de pénétration de créer, tester et déployer rapidement des campagnes de phishing.
- WARCannon : un outil permettant de rechercher les vulnérabilités du Web sur l'Internet, conçu pour les chercheurs en sécurité et les bug-hunters.
- Ping Castle : un outil permettant de réaliser des audits de sécurité sur les serveurs Active Directory.
- reNgine : un framework de reconnaissance automatique pour la collecte d'informations lors des pentest web.
- Racketeer : un outil permettant de simuler et de tester la détection d'opérations courantes de ransomware, de manière contrôlée.

Et bien d'autres qui peuvent été consultés sur le lien de la source.

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

Eavesdropping dans les applications de messagerie

05 Août 2021

Après la vulnérabilité de Facetime 2019, Silvanovich, une chercheuse de l'équipe de bug hunter du projet Zero de Google, a réussi à trouver d'autres vulnérabilités similaires dans plusieurs applications de messagerie.

Lors de la conférence Black Hat sur la sécurité, Silvanovich a exposé ses découvertes concernant des bugs d'écoute à distance dans des applications de communication omniprésentes comme Signal, Google Duo et Facebook Messenger, ainsi que dans les plateformes internationales JioChat et Viettel Mocha. Les vulnérabilités découvertes offraient un ensemble d'options d'écoute, comme par exemple le bug Facebook Messenger qui permet d'écouter l'appareil d'une cible. Les bugs Viettel Mocha et JioChat donnaient tous deux un accès avancé à l'audio et à la vidéo. La faille de Signal n'expose que l'audio. Et la vulnérabilité de Google Duo donne un accès vidéo, mais seulement pendant quelques secondes.

Il est important de préciser que toutes les failles ont été corrigées peu de temps après avoir été signalées.

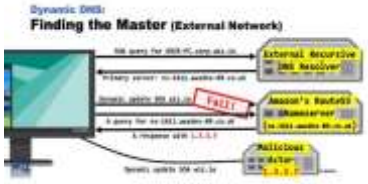
Sources *: https://bit.ly/3BdJ27v*

Un nouveau mécanisme d'espionnage DNS

4 août 2021

Toujours dans l'évènement Black Hat USA, les chercheurs de Wiz ont présenté une nouvelle vulnérabilité, qui expose les données DNS dynamiques. Cette vulnérabilité permet

d'intercepter une partie du trafic DNS dynamique lorsqu'il passe par des fournisseurs de DNS comme Amazon et Google. La cause du problème réside dans l'implémentation non standard des résolveurs DNS.



Il s'agit d'un vecteur de menace toujours actif car bien que deux grands fournisseurs de DNS (Amazon et Google) ont corrigé le problème, d'autres peuvent encore être vulnérables. Par conséquent, des millions d'appareils sont potentiellement vulnérables. Suite à l'exploitation de la vulnérabilité, plusieurs informations peuvent être interceptées telles que des adresses IP internes et externes, des noms d'ordinateurs et parfois des tickets NTLM / Kerberos.

L'équipe de recherche Wiz a également mis en ligne un outil qui permet aux entreprises de vérifier si leurs actualisations DNS internes sont transmises aux prestataires ou à des malfaiteurs.

Source : https://bit.ly/3gGO04S

Google Allstar : Un outil qui aide les développeurs à renforcer la sécurité

11 Août 2021

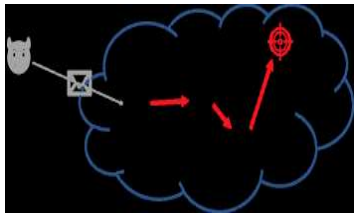
Google a annoncé sa dernière réalisation pour les développeurs, un outil qui automatise les tâches de sécurité et vérifie les attributs du projet pour s'assurer que la sécurité d'un projet open-source n'a pas changé. Nommé AllStar, l'outil utilise l'API GitHub pour vérifier l'état actuel du projet, les paramètres de la branche de développement et d'autres attributs afin de s'assurer que les aspects critiques du projet n'ont pas été modifiés.

"Allstar est utile lorsque votre projet ou votre organisation s'étend sur de nombreux référentiels et qu'il est trop compliqué de s'assurer que les bons paramètres et les bonnes pratiques sont configurés sur chaque référentiel", explique Jeff Mendoza, responsable de l'ingénierie d'Allstar pour Google.

Source : *https://bit.ly/3sGq9qF*

Hopper : Un outil de Dropbox pour détecter les attaques par mouvement latéral contre les réseaux d'entreprises

03 Août 2021



Hopper est un outil d'apprentissage automatique présenté dans une publication académique qui sera présenté à l'évènement Usenix Security Symposium le mois prochain. Cet outil, conçu par des chercheurs de Dropbox, de l'université de Berkeley et d'autres organisations, propose une nouvelle approche pour détecter les activités malveillantes dans les réseaux d'entreprises, permettant de détecter les attaques par mouvements latéral tout en réduisant le nombre de fausses alertes de sécurité.

Les chercheurs ont testé Hopper sur 15 mois de données provenant du réseau d'entreprise de Dropbox, composées de plus de 780 millions d'événements de connexion incluant 326 attaques simulées par une RedTeam. L'outil a été capable de détecter 94,5 % des attaques tout en produisant huit fois moins de fausses alarmes que les autres outils de détection des mouvements latéraux.

Source : *https://bit.ly/3ms4gdo*

Cloud… soyons prêts !

Etablir les indicateurs de performance clés pour la migration vers le Cloud

Les indicateurs de performance clés ou KPIs sont des indicateurs d'une application ou d'un service établis pour évaluer ses performances par rapport aux attentes.
Les meilleurs indicateurs de performance clés pour une migration vers le cloud devraient montrer les progrès de la migration en cours et révéler tout problème inattendu. De plus, ces indicateurs peuvent aider à déterminer à quel moment la migration est terminée et réussie.

Il existe plusieurs catégories fondamentales de KPI pour la migration vers le cloud. Voici quelques exemples :

- **Expérience utilisateur** : Temps de chargement des pages, Décalage, Temps de réponse, Durée de la session, etc.
- **Performance de l'application/du service** : Taux d'erreur, Débit, Disponibilité, etc.
- **Infrastructure** : Utilisation du processeur (%), Performance du disque, Utilisation de la mémoire, Débit du réseau, etc.
- **Engagement des clients** : Nouveaux clients, Taux d'engagement, etc.

Pour chaque catégorie, il faut déterminer les métriques les plus importantes pour l'entreprise et celles qui seront les plus impactées par la migration vers le cloud.

Source : *https://bit.ly/3zJY8ab*

Bon à savoir !

Paiement électronique : bonnes pratiques

Le paiement électronique est devenu une tendance mondiale ces dernières années. Les gens en bénéficient pour effectuer des tâches quotidiennes à distance, que ce soit pour faire des achats ou pour payer des factures en ligne.

En Algérie, en effet le domaine du paiement électronique commence tout juste à faire son apparition. Désormais, grâce aux cartes bancaires et postales (ex. Edahabia) et à leurs applications mobiles, les gens peuvent payer leurs factures, recharger leurs crédits téléphoniques et même faire certains achats. Et bien sûr avec ce progrès, il faut prendre en compte le risque de mettre ses identifiants en ligne, étant donné que les dernières statistiques montrent qu'entre 2019 et 2020, le nombre de rapports d'usurpation d'identité par cartes de crédit dans le monde a augmenté de 44,6 %.

Par conséquent, les personnes ayant l'intention d'utiliser des méthodes de paiement électronique doivent prendre des précautions et protéger leurs informations. Pour cela, quelques bonnes pratiques et mesures peuvent être appliquées pour prévenir le vol de vos identifiants :

- Gardez vos informations d'identification privées : ne les partagez avec personne, ne les saisissez pas devant les autres, et n'envoyez pas les détails de votre carte de crédit par courriel ou sur les réseaux sociaux.
- Ne stockez pas vos informations d'identification dans le navigateur, car ce dernier peut être vulnérable, et garder le navigateur à jour.
- Ne communiquez vos données que sur des sites sécurisés et de confiance. Vérifiez la présence d'une connexion https et de certificats de sécurité valides.
- N'introduisez pas votre identification sur des sites suspects, car il pourrait s'agir d'une attaque de phishing.
- N'utilisez pas vos identifiants dans un dispositif ou un réseau public ou non sécurisé.
- Vérifiez fréquemment les activités et les transactions effectuées sur votre compte pour détecter les activités suspectes au plutôt.

***Sources** : https://intuit.me/2UKbqhV ; https://bit.ly/3860Ip0*

Evènements

Evènements du mois

CISO Online, A/NZ

17-18 Août 2021

Online

https://bit.ly/3gscTB5

Dans la 3ème édition de CISO Online - A/NZ, les intervenants ont présenté durant 2 jours, les outils et les meilleures pratiques pour suivre l'innovation technologique en abordant divers sujets tels que :

- La gestion des incidents de cybersécurité.
- La gestion des risques.
- La gestion des identités.
- Méthodes pour améliorer la culture et la sensibilisation vis à vis de la cybersécurité.
- La protection des données.
- Blockchain pour la cybersécurité.
- La sécurité de l'IoT.

Evènements à venir

Virtual Cybersecurity & Fraud Summit : London

14-15 Septembre 2021

Online

https://bit.ly/3gz6zb4

La communauté mondiale d'experts en sécurité et en conformité de l'ISMG va se réunir dans le cadre de cet évènement pour offrir des conférences sur plusieurs thématiques essentielles dans le domaine de la cybersécurité, comme la prévention des fraudes et des violations, le concept de Zero-trust et les défis spécifiques au secteur.

Référence	ANPT-2021-BV-08
Titre	Bulletin de veille N°08
Date de version	31 Août 2021
Contact	ssi@anpt.dz