BULLETIN DE VEILLE N°10

ANPT-2021-BV-10

« Understand what data you hold, how you are using it, and make sure you are practicing good data hygiene. » *-David Mount-*

Octobre 2021

Alertes de sécurité

Android

Une nouvelle mise à jour pour corriger des vulnérabilités de haute gravité

05 Octobre 2021

Google a publié une mise à jour pour corriger plusieurs vulnérabilités de haute gravité trouvées dans Android. Parmi ces vulnérabilités nous trouvons :

- CVE-2021-0703 : Une vulnérabilité qui permet à un attaquant local disposant d'un accès physique à l'appareil d'exécuter du code arbitraire.
- CVE-2021-0483 : une vulnérabilité qui pourrait permettre à une application locale malveillante d'exécuter du code arbitraire dans le contexte d'un processus privilégié.
- CVE-2021-0643 et CVE-2021-0706 : Deux vulnérabilités permettant à un attaquant local disposant d'un accès privilégié d'accéder à des données sensibles.

Plus de détails peuvent être consultés dans le bulletin de sécurité d'Android.

Source : *https://bit.ly/2XPf23A*

Adobe

Des correctifs urgents pour les produits Adobe

26 Octobre 2021

Adobe a publié des correctifs urgents pour plus de 90 vulnérabilités. 61 vulnérabilités d'exécution de code arbitraire et 05 de fuites de mémoire ont été qualifiées de "critiques".

Ces bugs de sécurité affectent un large éventail de produits populaires, notamment Adobe Photoshop, Adobe InDesign, Adobe Illustrator et Adobe Premiere.

Adobe a publié des avis contenant des détails sur les vulnérabilités présentes dans Adobe After Effects (11 vulnérabilités), Audition (9), Bridge (9), Character Animation (8), Prelude (9), Lightroom Classic (1), Illustrator (5), Media Encoder (6), Premiere Pro (6), Animate (10), Premiere Elements (7), InDesign (3), XMP Toolkit SDK (5) et Photoshop (3).

La société affirme n'avoir connaissance d'aucune attaque exploitant ces vulnérabilités, cependant, l'application des correctifs est primordiale pour se protéger d'éventuelles exploitations futures.

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

ZTE

Multiples vulnérabilités dans le routeur LTE ZTE MF971R

18 Octobre 2021

Cisco Talos a récemment découvert de multiples vulnérabilités dans le routeur portable LTE ZTE MF971R.

Deux problèmes parmi ceux découvert représentent des vulnérabilités de dépassement de tampon basées sur la pile. Un attaquant pourrait exploiter ces problèmes pour exécuter du code arbitraire à distance sur le périphérique ciblé.

Deux autres sont des vulnérabilités XSS de pré-authentification qu'un attaquant pourrait utiliser pour exécuter un code JavaScript arbitraire dans le navigateur de la victime dans le contexte d'un panneau Web de routeur. Dans ce cas, l'attaquant doit inciter l'utilisateur à ouvrir une URL contrôlée par l'attaquant qui héberge la requête HTTP malveillante.

De plus, une faille peut être exploitée pour provoquer un écrasement des entrées du fichier de configuration, ce qui, dans certains cas, pourrait permettre à l'attaquant de verrouiller complètement le périphérique.

Et enfin, une vulnérabilité d'injection de CRLF dans le routeur qui est une combinaison de CVE-2021-21748 (débordement de tampon basé sur la pile avant authentification) et de CVE-2021-21745 (contournement de la vérification CSRF/Referer) qui, ensemble, permettent à un attaquant de déclencher un code

arbitraire à distance sur le dispositif vulnérable sans aucune authentification.

Ces problèmes sont résolus dans la dernière mise à jour.

Les utilisateurs sont encouragés à mettre à jour ces produits affectés dès que possible.

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

Microsoft

Deux vulnérabilités dans PowerShell 7 permettant le contournement de WDAC

14 Octobre 2021

Microsoft a corrigé deux vulnérabilités dans PowerShell 7, permettant aux attaquants de contourner les mesures d'application de Windows Defender Application Control (WDAC) et d'accéder à des informations d'identification en texte clair.

WDAC est conçu pour protéger les appareils Windows contre les logiciels potentiellement malveillants en veillant à ce que seuls les applications et les pilotes de confiance puissent s'exécuter, bloquant ainsi le lancement de logiciels malveillants et indésirables.

En exploitant la vulnérabilité de contournement de la fonction de sécurité Windows Defender Application Control, connue sous le nom de CVE-2020-0951, les acteurs de la menace peuvent contourner la liste des autorisations de WDAC, ce qui leur permet d'exécuter des commandes PowerShell qui seraient autrement bloquées lorsque WDAC est activé.

La deuxième faille, connue sous le nom de CVE-2021-41355, est une vulnérabilité de divulgation d'informations dans .NET Core, où les informations d'identification pourraient être divulguées en texte clair sur des appareils fonctionnant sur des plateformes autres que Windows.

La vulnérabilité CVE-2020-0951 affecte les versions PowerShell 7 et PowerShell 7.1, tandis que CVE-2021-41355 n'affecte que les utilisateurs de PowerShell 7.1.

Il est conseillé aux administrateurs d'installer les versions mises à jour de PowerShell 7.0.8 et 7.1.5 dès que possible afin de protéger les systèmes contre les attaques potentielles.

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

Patch Tuesday de Microsoft

12 Octobre 2021

Dans le cadre du Patch Tuesday de ce mois, Microsoft a publié les corrections pour un total de 74 failles (81 en comptant Microsoft Edge).

Parmi ces vulnérabilités, nous trouvons 21 vulnérabilités d'élévation de privilèges, 6 vulnérabilités de contournement des fonctions de sécurité, 20 vulnérabilités d'exécution de code à distance, 13 vulnérabilités de divulgation d'informations, 5 vulnérabilités de déni de service et 9 vulnérabilités liées à l'usurpation d'identité.

Ce Patch comprend des correctifs pour quatre vulnérabilités de type Zero day, dont une vulnérabilité Win32k d'élévation de privilège (CVE-2021-40449) connue pour avoir été activement exploitée dans la nature.

Les trois autres failles Zero Day corrigées sont une vulnérabilité d'exécution de code à distance du serveur DNS de Windows (CVE-2021-40469), une vulnérabilité d'élévation de privilège du noyau Windows (CVE-2021-41335) et un problème de contournement de la fonctionnalité de sécurité des règles du pare-feu Windows AppContainer (CVE-2021-41338).

Le reste des bugs corrigés sont listé ici.

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

Node.js

Node.js fait face à deux nouvelles vulnérabilités

12 Octobre 2021

Les mainteneurs de Node.js ont corrigé deux vulnérabilités de type HTTP request smuggling (HRS) dans l'environnement d'exécution JavaScript. Une attaque à distance non authentifiée pourrait les exploiter pour contourner les contrôles de sécurité, obtenir un accès non autorisé à des données sensibles et compromettre d'autres utilisateurs de l'application.

Le premier problème, nommé CVE-2021-22959, permet la contrebande de requêtes HTTP en raison des espaces dans les en-têtes, l'analyseur HTTP acceptant les requêtes avec un espace après le nom de l'en-tête et avant les deux points.

Cependant, la deuxième faille, CVE-2021-22960 semble représenter une nouvelle technique HRS, par laquelle la combinaison d'une mauvaise terminaison de ligne dans l'un des proxys étudiés et d'une analyse incorrecte des extensions de chunk dans Node permet la contrebande de requêtes.

"Ces deux problèmes combinés nous permettent de construire un corps en morceaux que le mandataire interprète d'une certaine manière et que Node interprète d'une autre manière. Nous avons également constaté le même comportement du serveur dans trois autres serveurs que nous avons étudiés, ce qui fait de ce problème le plus grave que nous ayons trouvé."

Node a publié un correctif pour ces vulnérabilités et invite tous les utilisateurs de l'appliquer dès que possible.

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

IBM

Une vulnérabilité touche plusieurs produits IBM

12 Octobre 2021

Une vulnérabilité a été découverte dans plusieurs produits IBM. Elle pourrait permettre à un attaquant authentifié d'obtenir des informations sensibles et de provoquer un déni de service.

Répertoriée CVE-2021-29873, le problème concerne plusieurs produits exécutant les versions 7.8 à 8.4 prises en charge.

IBM recommande de corriger cette vulnérabilité en mettant à jour les produits listés dans son bulletin de sécurité aux dernières versions.

Sources : *https://bit.ly/3bdJ583*

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

Actualité

Les applications "Squid Game" contaminent les appareils avec des malwares

25 Octobre 2021

La tendance du Squid Game ne semble pas vouloir disparaître bientôt, du moins pas pour l'instant. Le 19 de ce mois, Lukas Stefanko – un chercheur chez ESET- a indiqué sur Twitter que plus de 200 applications liées à Squid Game sont disponibles sur Google Play, ce qui constitue une excellente occasion de gagner de l'argent avec les publicités intégrées dans les applications. Il a également précisé que la plus téléchargée de ces applications a atteint 1 million d'installations en 10 jours. Parallèlement à la popularité de ces applications, une hausse du nombre d'escroqueries a été perçue. Car comme toujours les cybercriminels tentent de tirer profit des fans peu méfiants.

Selon Lukas Stefanko, une des applications qui est censée servir de fond d'écran à Squid Game installait le logiciel malveillant "Joker" sur des appareils Android. Le chercheur a signalé le problème à Google après l'avoir détecté.

L'application a été téléchargée au moins 5 000 fois avant que Google ne la supprime.

Le malware Joker est bien connu et peut permettre aux pirates d'inscrire les utilisateurs à des services payants très coûteux dont ils peuvent tirer profit.

L'application a actuellement été retirée du Play Store. Mais les utilisateurs inactifs qui l'ont installé doivent la désinstaller instantanément de leurs appareils.

Sources *: https://bit.ly/3BkdRH3 ; https://bit.ly/3Gun8Ad*

Facebook : un nouvel outil pour détecter les vulnérabilités SSRF

22 Octobre 2021

Facebook a mis en place un nouvel outil pour aider les chercheurs en sécurité dans leur chasse aux vulnérabilités de type SSRF (Server-Side Request Forgery).

Une attaque SSRF peut permettre à un attaquant d'accéder ou de modifier des ressources internes en abusant les capacités d'un serveur. En exploitant cette dernière, un attaquant peut être en mesure de lire la configuration du serveur, comme les métadonnées AWS (Amazone web services), de se connecter à des services internes, comme les bases de données http, ou d'effectuer des requêtes vers des services internes qui ne sont pas censés être exposés.

Cet outil, baptisé SSRF Dashboard, possède une interface utilisateur simple qui permet aux chercheurs de définir des URLs internes uniques pour le ciblage, puis de déterminer si ces URLs ont été atteintes lors d'une tentative de SSRF. Il fournit la date de création, un identifiant unique et le nombre de visites que l'URL a reçues, en plus de l'URL unique de tentative SSRF créée, qui est présentée dans un tableau avec d'autres URLs.

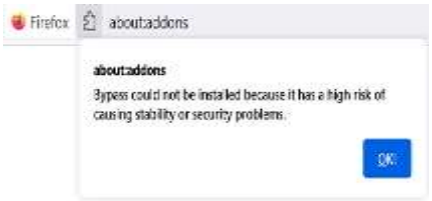
Selon Facebook, grâce à ce nouvel outil, les chercheurs en sécurité peuvent déterminer avec précision si leur code de preuve de concept (PoC) SSRF a réussi, car seuls les PoC réussis reçoivent des visites.

Source *: https://bit.ly/3CjmuD4*

Mozilla Firefox : Des modules complémentaires malveillants empêchent le navigateur de télécharger les mises à jour de sécurité

25 Octobre 2021

Mozilla a révélé qu'elle avait bloqué deux extensions Firefox malveillantes installées par 455 000 utilisateurs, qui utilisaient abusivement l'API Proxy pour empêcher le téléchargement des mises à jour du navigateur. Étant donné que l'API Proxy peut être utilisée pour acheminer des requêtes web, un abus de l'API pourrait permettre à un mauvais acteur de contrôler efficacement la manière dont le navigateur Firefox se connecte à l'internet.



Les deux extensions en question, nommées "Bypass" et "Bypass XM", ont empêché les utilisateurs qui les avaient installées de télécharger des mises à jour, d'accéder à des listes de blocage actualisées et de mettre à jour du contenu configuré à distance.

En plus de bloquer ces extensions, Mozilla a déclaré qu'elle suspendait les autorisations pour les nouveaux modules complémentaires qui utilisent l'API du proxy jusqu'à ce que les correctifs soient largement disponibles. De plus, Mozilla a ajouté qu'elle avait déployé un module complémentaire appelé "Proxy Failover" qui comporte des mesures d'atténuation supplémentaires pour résoudre le problème.

Les usagers qui ont installé les modules complémentaires problématiques sont invités à les supprimer en se rendant dans la section Add-ons et en recherchant explicitement "Bypass" (ID : 7c3a8b88-4dc9-4487-b7f9-736b5f38b957) ou "Bypass XM" (ID : d61552ef-e2a6-4fb5-bf67-8990f0014957).

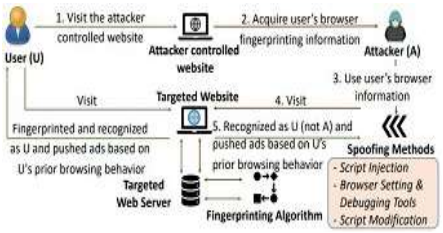
Source *: https://mzl.la/3Gyqm5U*

Gummy browsers : une attaque qui permet d'usurper vos identités numériques

20 Octobre 2021

Une nouvelle attaque de capture d'empreintes digitales et d'usurpation de navigateur, baptisée Gummy Browsers, a été

développée par des chercheurs universitaires américains. Il s'agit d'une attaque facile à réaliser mais dont les conséquences sont graves.



Cette technique d'attaque peut être utilisée pour contourner le système 2FA des systèmes d'authentification une fois que l'attaquant a obtenu les empreintes digitales via son site web malveillant.

Les résultats de la recherche ont démontré que les Gummy Browsers peuvent réussir à usurper l'identité du navigateur de la victime presque à chaque tentative, sans pour autant affecter la traçabilité des utilisateurs légitimes.

L'attaque "Gummy Browsers" consiste à capturer l'empreinte digitale d'une personne en lui faisant visiter un site web contrôlé par l'attaquant, puis à utiliser cette empreinte sur une plate-forme cible pour usurper l'identité de cette personne. Après avoir généré l'empreinte digitale d'un utilisateur à l'aide de scripts de spoofing existants ou personnalisés, les chercheurs ont déclaré qu'ils pouvaient tromper les systèmes d'empreintes digitales de pointe tels que FPStalker et Panopliclick pendant de longues périodes.

Les chercheurs ont averti que l'impact de l'attaque Gummy Browsers peut être dévastateur et durable sur la sécurité en ligne et la vie privée des utilisateurs, d'autant plus que l'empreinte digitale du navigateur commence à être largement adoptée dans le monde réel.

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

Un décrypteur pour le ransomware BlackMatter est maintenant disponible

24 Octobre 2021

Le fabricant d'antivirus et la société de cybersécurité Emsisoft a annoncé la disponibilité d'un utilitaire de décryptage gratuit pour les anciennes victimes du ransomware BlackMatter.

Après avoir identifié la faille de chiffrement plus tôt cet été, Emsisoft avait travaillé avec des agences gouvernementales et des organismes d'application de la loi pour atteindre les anciennes victimes de BlackMatter et distribuer le décrypteur via des canaux privés, afin de les aider à récupérer leurs fichiers sans avoir à payer d'énormes rançons. Sachant que les opérateurs de BlackMatter ont déjà atteint de nombreuses organisations basées aux États-Unis et ont exigé le paiement de rançons allant de 80 000 à 15 000 000 $ en Bitcoin et Monero.

Le directeur technique d'Emsisoft a déclaré qu'ils ont annoncé publiquement le décrypteur aujourd'hui comme un moyen d'atteindre les victimes de BlackMatter qu'ils n'ont pas pu identifier et contacter, et qu'ils n'ont pas révélé l'existence de la faille avant pour éviter que le groupe ransomware répare le code de leur malware.

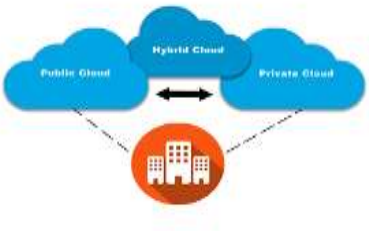
Le décrypteur ne permet de décrypter que les fichiers chiffrés avec les versions de BlackMatter utilisées entre la mi-juillet et la fin septembre 2021, étant donné que le problème a été résolu par la version la plus récente du ransomware.

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

Cloud… soyons prêts !

Comprendre vos options de déploiement : cloud public, cloud privé ou cloud hybride ?

Il existe trois façons différentes de déployer des services de cloud computing : sur un cloud public, un cloud privé ou un cloud hybride. Le choix de la méthode de déploiement dépend des besoins des entreprises.



- Dans un cloud public, les ressources du nuage sont détenues et exploitées par un fournisseur de services cloud. Les organisations utilisant ce type de nuage partagent ces ressources (matériel, stockage, périphériques réseau), accèdent à leurs services et gèrent leurs comptes via les navigateurs Web. Les avantages des clouds publics sont la réduction des coûts et l'évolutivité quasi illimitée.
- Dans le cloud privé, les services et l'infrastructure sont maintenus sur un réseau privé et le matériel et les logiciels sont dédiés uniquement à une organisation, ce qui accorde plus de sécurité et lui permet de personnaliser plus facilement ses ressources pour répondre à ses besoins.
- Un cloud hybride est un type de cloud computing qui combine un cloud privé avec un cloud public afin de tirer les avantages de chacun. Les clouds hybrides permettent aux données et aux applications de circuler entre les deux environnements. Son principal avantage réside dans la possibilité de maintenir une infrastructure privée pour les actifs sensibles ou les charges de travail qui nécessitent une faible latence et une infrastructure public pour le reste des services.

Source : *https://bit.ly/3Bin0QI*

Bon à savoir !

Les scams en ligne : Signes & Prévention

« **Si c'est trop beau pour être vrai, ça ne l'est probablement pas** », cette citation est parfaitement placée lorsque nous abordons le sujet des scams (escroqueries). Dans la vie réelle ou en ligne, les fraudeurs tentent toujours de trouver de nouvelles approches pour se servir et tirer profiter des gens, qui qu'ils soient, étant donné que les escrocs ne visent pas nécessairement une catégorie spécifique. Particulièrement depuis que l'internet est devenu un outil essentiel dans notre vie quotidienne, les escrocs se lancent dans l'arnaque en ligne.

Afin de prévenir la fraude en ligne, vous devez être conscient des signes que montrent les escrocs. Par exemple, si une personne que vous ne connaissez pas ou une organisation vous contacte de manière inattendue ou si elle vous demande de l'argent quel que soit manière, ou des informations personnelles ou financières, vous devez être alertés. Car les arnaqueurs ne laissent aucune chance ou opportunité sans la saisir.

Bien heureusement, il existe de nombreux moyens simples pour vous protéger, parmi lesquelles nous allons en mentionner quelques-unes ci-dessous :

- Ne cliquez pas sur des liens ou ne téléchargez pas de pièces jointes provenant d'expéditeurs que vous ne connaissez pas ;
- Faites toujours des recherches sur les personnes ou les organisations qui vous demandent des informations et confirmez qu'elles sont dignes de confiance avant de divulguer des données personnelles ;
- Maintenez vos logiciels à jour ;
- Utilisez des mots de passe forts et envisagez d'utiliser un gestionnaire de mots de passe pour les créer et stocker en toute sécurité ;
- Souscrivez à un système de sécurité (antivirus) pour protéger votre appareil contre les menaces, les virus, les logiciels malveillants et les logiciels espions.

Surtout, faites preuve de bon jugement lorsque vous utilisez l'internet et restez attentif aux menaces de sécurité lorsque vous utilisez votre téléphone, votre ordinateur ou tout autre appareil.

Sources : *https://bit.ly/3vQ2BBf*

Evènements

Evènement du mois

MCTF

20 - 26 Octobre 2021

Online

https://bit.ly/3mjSwt9

Le Micro club de l'USTHB en collaboration avec le club Shellmate de l'ESI ont lancé un défi virtuel de capture du drapeau (CTF). Différents challenges liés à des problèmes de sécurité informatique et/ou de capture et de défense de systèmes informatiques ont été exposés aux participants pour les résoudre pendant deux jours. Par la suite, deux webinaires ont été présentés, le premier était intitulé « How to become a world class cybersecurity professional » et le second « Best practices to secure your containers ».

Evènement à venir

Cyber Security Awareness - Workshop

04 Novembre 2021

Online

https://bit.ly/3jJBQd0

Ce workshop sur la cybersécurité vise à aider les organisations à réduire les risques liés à la cybercriminalité de manière systématique et cohérente en offrant des conseils pratiques sur l'identification des risques, la mise en œuvre de contrôles de sécurité en matière de protection et de détection, ainsi que sur les moyens de répondre aux incidents de sécurité et de s'en remettre.

Référence	ANPT-2021-BV-10
Titre	Bulletin de veille N°10
Date de version	31 Octobre 2021
Contact	ssi@anpt.dz