
# BULLETIN DE VEILLE N°11

ANPT-2020-BV-11

« Il y a bien des manières de ne pas réussir, mais la plus sûre est de ne jamais prendre de risques. » -Benjamin Franklin-

Novembre 2020

# Alertes de sécurité

## Google

### Google corrige deux autres 0-day pour Chrome

11 novembre 2020

Google a publié la version 86.0.4240.198 de Chrome pour corriger deux vulnérabilités zero-day qui ont été exploitées dans la nature.

Selon le journal des modifications Chrome 86.0.4240.198, la première vulnérabilité référencée CVE-2020-16013 est décrite comme une « implémentation inappropriée dans V8 », où V8 est le composant Chrome qui gère le code JavaScript.

La seconde faille CVE-2020-16017 est un bug de corruption de mémoire « use after free » dans « Site Isolation » , le composant Chrome qui isole les données de chaque site les unes des autres.

Il est actuellement inconnu si les deux vulnérabilités ont été utilisées ensemble, dans le cadre d'une chaîne d'exploitation, ou utilisées individuellement.

Deux autres vulnérabilités zero-day ont été corrigées le 02 novembre. La faille référencée CVE-2020-16009, également dans le moteur JavaScript V8 de Chrome, et la faille référencée CVE-2020-16010 cette fois dans Chrome pour Android, impactant le composant d'interface utilisateur (UI) du navigateur.

Il est conseillé d'appliquer les dernières mises à jour publiées par Google.

***Source*** *: https://zd.net/2J2zZR5*

## Linux

### Ubuntu corrige des bugs permettant aux utilisateurs standards d'avoir les droits root

11 novembre 2020

Les développeurs Ubuntu ont corrigé une série de vulnérabilités qui permettraient aux utilisateurs standards d'obtenir facilement des privilèges root convoités.

Un chercheur en sécurité a accidentellement réussi à élever les privilèges locaux (LPE) sur le système d'exploitation Ubuntu en enchaînant l'exploit de deux vulnérabilités pour obtenir un accès root.

La première vulnérabilité référencée CVE-2020-16126 de type déni de service réside dans le démon AccountsService, un démon qui gère les comptes utilisateurs.

La seconde vulnérabilité référencée CVE-2020-16125 est une vulnérabilité d'élévation de privilèges dans GNOME Display Manager en raison d'une absence de réponse du démon de comptes.
Linux étant le système d'exploitation le plus populaire pour serveur, il est donc possible que les composants du bureau aient été moins examinés.

Dans l'ensemble, d'autres bonnes raisons de garder les systèmes patchés et de ne pas installer une interface graphique sur un serveur.

***Source:*** *https://bit.ly/33bFJ0p*

## Cisco

### Une faille Cisco Webex Meetings permet à n'importe qui de rejoindre une session Webex

19 novembre 2020

Cisco a corrigé une faille au sein de la plate-forme de visioconférence Cisco Webex. Cette vulnérabilité est due à une mauvaise gestion des jetons d'authentification par un site Webex vulnérable.

«Un participant non autorisé pourrait exploiter cette vulnérabilité en accédant à un ID de réunion connu ou à une URL de réunion à partir du navigateur de l'appareil mobile. Le navigateur demandera alors de lancer l'application mobile Webex de l'appareil », a écrit Cisco dans un avis publié dans Cisco Security Advisory. L'intrus peut accéder, par la suite, à la réunion sans apparaître sur la liste des participants, aucun mot de passe n'étant requis.

Cette vulnérabilité affectait tous les sites Cisco Webex Meetings avant le 17 novembre 2020. Au moment de la publication, cette vulnérabilité affectait également toutes les applications Cisco Webex Meetings versions 40.10.9 et antérieures pour iOS et Android.

Les versions 40.11 et ultérieures de l'application mobile Cisco Webex Meetings contenaient le correctif de cette vulnérabilité.

Cisco a corrigé cette vulnérabilité sur les sites Cisco Webex Meetings, qui sont basés sur le cloud.

***Source :*** *https://bit.ly/372MHY0*

## Microsoft

### Le Microsoft patch Tuesday de Novembre 2020 arrive avec un correctif pour Microsoft Zero-Day

16 novembre 2020

Les correctifs publiés de ce mois-ci dans le patch Tuesday incluent également un correctif pour une vulnérabilité Windows zero-day référencée CVE-2020-17087 qui a été exploitée dans la nature.

Le zero-day de Windows a été utilisé dans le cadre d'une attaque qui exploitait en même temps un autre zero-day de Chrome référencé CVE-2020-15999. La vulnérabilité de Chrome a été utilisé pour permettre aux attaquants d'exécuter du code malveillant dans Chrome, tandis que la vulnérabilité de Windows était la deuxième partie de cette attaque, permettant aux acteurs menaçants d'échapper au conteneur sécurisé de Chrome et d'exécuter du code sur le système d'exploitation sous-jacent - dans ce que les experts en sécurité appellent une évasion sandbox.

Selon l'avis de sécurité de Microsoft pour CVE-2020-17087 , le 0-day réside dans le noyau Windows et affecte toutes les versions actuellement prises en charge du système d'exploitation Windows. Cela inclut toutes les versions après Windows 7 et toutes les distributions de Windows Server.

Mais en plus du 0-day de Windows, 111 autres vulnérabilités doivent également être corrigées.

***Source :*** *https://zd.net/3mkbQEe*

### Microsoft corrige un bug d'authentification Kerberos

17 novembre 2020

Microsoft travaille sur la correction d'un bug causé par le patch de la semaine dernière. Celui-ci corrigeait une vulnérabilité de contournement dans la fonction de sécurité du centre de distribution de clés Kerberos (Key Distribution Center, KDC).

Microsoft signale que le problème affecte les systèmes qui ont installé le correctif pour la vulnérabilité CVE-2020-17049.

Selon Microsoft, le correctif défectueux ne concerne que les serveurs Windows, les appareils Windows 10 et les applications dans les environnements d'entreprise.

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

## Oracle

### Un correctif d'urgence pour WebLogic Server

09 novembre 2020

Le nouveau patch corrige une vulnérabilité critique référencée CVE-2020-14750 d'exécution de code à distance (RCE) affectant plusieurs versions d'Oracle WebLogic Server.

Cette faille peut être exploitée par un pirate sans nécessiter une quelconque authentification. Dans ce cadre, Oracle a publié une alerte de sécurité le 01 Novembre afin de signaler que ce premier patch n'arrive pas à corriger entièrement la faille

À défaut, il est recommandé de désactiver temporairement la console WebLogic.

***Source :*** *https://bit.ly/37jEMWE*

## WordPress

### Vulnérabilité RCE authentifiée dans le plugin WordPress Secure File Manager (non corrigé).

23 novembre 2020

Le plugin WordPress Secure File Manager (± 1000 installations actives) est sujet à une vulnérabilité d'exécution de code à distance authentifiée affectant la version 2.5 et inférieure.

Tout utilisateur connecté peut exécuter les commandes du gestionnaire de fichiers (par exemple, télécharger, renommer, créer, afficher, supprimer, etc.). La commande peut être exécutée dans n'importe quel répertoire à l'intérieur du vhost.

Nous vous recommandons de désinstaller ce plugin car aucun correctif de sécurité n'est encore disponible.

***Source :*** *https://bit.ly/2KH34lM*

## VMware

### VMware corrige de graves vulnérabilités dans l'hyperviseur ESXi, SD-WAN Orchestrator

20 novembre 2020

VMware a corrigé des vulnérabilités critiques affectant son hyperviseur ESXi de classe entreprise.

Deux vulnérabilités référencée CVE-2020-4004 et CVE-2020-4005 ont été exploité lors d'un concours « Tianfu Cup Pwn » qui a eu lieu à Chengdu, en Chine.

La première faille est une vulnérabilité « use after free », les attaquants peuvent l'exploiter pour disposer de privilèges administratifs locaux sur une machine virtuelle pour l'exécution du code en tant que processus VMX de la machine virtuelle s'exécutant sur l'hôte. La seconde faille est une vulnérabilité d'élévation de privilèges VMX pouvant être utilisée par des attaquants qui disposent de privilèges dans le processus VMX pour élever leurs privilèges sur le système affecté.

Les utilisateurs sont invités à lire attentivement cet avis et à voir s'ils doivent mettre à jour leurs installations.

VMware a également publié une mise à jour de sécurité pour son orchestrateur SD-WAN, comblant une poignée de failles de sécurité graves.

***Source:*** *https://bit.ly/35TrP6e*

# Actualité

## L'empoisonnement du cache DNS, l'attaque Internet de 2008, est de retour d'entre les morts

12 novembre 2020


En 2008, le chercheur Dan Kaminsky a révélé l'une des menaces de sécurité Internet les plus graves jamais vues : une faiblesse dans le système de noms de domaine qui permettait aux attaquants d'envoyer en masse des utilisateurs vers des sites imposteurs au lieu des véritables sites demandés. Grâce à une coordination générale, des milliers de fournisseurs DNS du monde entier ont installé un correctif qui a évité ce scénario apocalyptique.

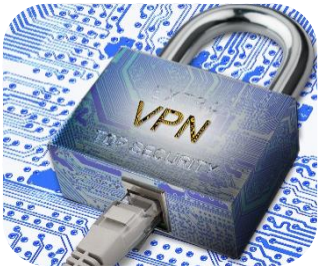
Maintenant, l'attaque d'empoisonnement du cache DNS de Kaminsky est de retour. Les chercheurs ont présenté mercredi une nouvelle technique qui peut à nouveau amener les résolveurs DNS à renvoyer des adresses IP frauduleuses au lieu du site qui correspond à juste titre à un nom de domaine […].

La recherche a été présentée lors de la conférence 2020 ACM sur la sécurité informatique et des communications. Les chercheurs fournissent des informations supplémentaires ici , et un communiqué de presse UC Riverside est ici .

***Source*** *: https://bit.ly/3kUK6Ve*

## Vulnérabilités VPN - Le cadeau qui continue d'offrir aux attaquants

27 novembre 2020




Les acteurs de la menace n'ont que l'embarras du choix alors que l'utilisation des services VPN augmente avec la pandémie du covid-19. Avec de nombreux employés travaillant toujours à domicile, l'utilisation de VPN a ouvert un pool d'attaques contre leurs utilisateurs.

Selon les statistiques, ZDNet a conclu que les Appliances VPN présentant de multiples vulnérabilités figuraient parmi les trois principaux vecteurs d'intrusion populaires utilisés au premier semestre 2020. Au cours du second semestre, l'intensité de ces attaques aurait augmenté à mesure que les acteurs menaçants ont canalisé leurs attaques via des exploits pour les produits VPN.

Plus tôt ce mois-ci, un pirate informatique a publié une liste d'adresses IP de près de 50000 périphériques VPN Fortinet vulnérables à une vulnérabilité de traversée de chemin (CVE-2018-13379).

Au cours de l'enquête, il a été constaté que les domaines ciblés appartenaient à des banques et à des organisations gouvernementales du monde entier.

Le VPN n'est pas une cible oubliée pour les cybercriminels. L'exploitation de VPN vulnérables peut permettre aux attaquants d'accéder aux réseaux internes d'une grande entreprise et les aider dans leur tentative d'obtenir un accès permanent à des ressources sensibles. Par conséquent, la sécurité des VPN est cruciale pour les entreprises, offrant un moyen sécurisé mais rentable d'utiliser Internet pour de nombreux besoins commerciaux essentiels.

***Source*** *: https://bit.ly/2Vgk9oK*

## Un pirate informatique vend l'accès aux comptes de messagerie de centaines de cadres de haut niveau

27 novembre 2020

Un pirate informatique vend actuellement des mots de passe pour les comptes de messagerie de centaines de cadres de haut niveau dans des entreprises du monde entier.

Les données sont vendues sur un forum clandestin à accès fermé pour les pirates russophones nommé *Exploit.in* […].

Selon les données fournies par la société de renseignement sur les menaces KELA , le même pirate avait précédemment exprimé son intérêt à acheter des « journaux Azor », un terme qui fait référence aux données collectées à partir d'ordinateurs infectés par le cheval de Troie voleur d'informations AzorUlt .

Les journaux d'Infostealer contiennent presque toujours des noms d'utilisateur et des mots de passe que le cheval de Troie extrait des navigateurs trouvés installés sur les hôtes infectés […].

Le moyen le plus simple d'empêcher les pirates de monétiser tout type d'informations d'identification volées est d'utiliser une solution de vérification en deux étapes (2SV) ou d'authentification à deux facteurs (2FA) pour vos comptes en ligne. Même si les pirates parviennent à voler les informations de connexion, ils seront inutiles sans le vérificateur supplémentaire.

***Source*** *: https://zd.net/37jJSC6*

## Microsoft met en garde contre les SMS et les appels vocaux pour l'authentification multifacteur

11 novembre 2020


Microsoft a conseillé les internautes d'adopter l'authentification multifacteur (MFA) ... sauf lorsque des réseaux téléphoniques publics commutés sont impliqués […].

Dans un article de blog , Alex Weinert, directeur de la sécurité d'identité chez Microsoft, déclare que les gens devraient absolument utiliser MFA. Il affirme que les comptes utilisant n'importe quel type de MFA sont compromis à un taux inférieur à 0,1% de la population générale.

En même temps, il soutient que les gens devraient éviter de se fier aux messages SMS ou aux appels vocaux pour gérer les

codes d'accès à usage unique (OTP), car les protocoles basés sur le téléphone sont fondamentalement non sécurisés.

Des informaticiens de l'Université de Princeton ont examiné l'échange de cartes SIM dans une étude de recherche [PDF ] plus tôt cette année et leurs résultats soutiennent les affirmations de Weinert. Ils ont testé AT&T, T-Mobile, Tracfone, US Mobile et Verizon Wireless et ont découvert que «les 5 opérateurs utilisaient des défis d'authentification non sécurisés qui pourraient facilement être contournés par des attaquants» […].

Pour ceux qui sont inquiets par plus de contrôle d'accès Microsoft, il existe des alternatives, comme Twilio's Authy, Duo Mobile de Cisco, Google Authenticator et des gestionnaires de mots de passe comme 1Password et LastPass. N'importe lequel de ces éléments constituerait une amélioration par rapport aux SMS et à la voix.

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

## Certaines applications Apple sur *macOS Big Sur* contournent le pare-feu et les VPN

17 novembre 2020

Les chercheurs en sécurité contredisent Apple pour une fonctionnalité de la dernière version Big Sur de macOS qui permet à certaines applications Apple de contourner le pare-feu et les VPN. Ils disent que c'est une vulnérabilité qui peut être exploitée par les cybercriminels pour contourner les pare-feu et leur donner accès aux systèmes des utilisateurs et exposer leurs données sensibles.

Le problème a été repéré pour la première fois le mois dernier par un utilisateur de Twitter nommé Maxwell, dans une version bêta du système d'exploitation.

Patrick Wardle, chercheur en sécurité chez Jamf, a confirmé que cela se produisait et a expliqué dans un commentaire que les précédentes versions de macOS permettaient de mettre en place un pare-feu ou un VPN en utilisant l'extension du noyau réseau (kext).

Dans un tweet, Wardle a montré comment les cybercriminels pouvaient utiliser des logiciels malveillants pour exploiter facilement la faille entre les applications Apple et les pare-feu des utilisateurs. Ce faisant, ils pourraient ensuite envoyer les données personnelles des utilisateurs à des serveurs distants, ce qui mettrait en danger à la fois leur vie privée et leur sécurité.

À l'heure actuelle, il est encore difficile de comprendre pourquoi Apple exempterait ses propres applications des pare-feu et des VPN. Certains pensent que cela est dû à des problèmes de licence, tandis que d'autres pensent que l'entreprise veut garder les données et le trafic de ses applications hors des serveurs VPN.

***Source :*** *https://bit.ly/3q1habX*

## Manchester United victime d'une cyberattaque

27 novembre 2020

Manchester United était victime d'une cyberattaque visant ses systèmes informatiques dont beaucoup restent hors ligne. Il a même été question d'une rançon demandée au club, selon le Daily Mail, un journal national britannique.

Le porte-parole du club ne se prononcera pas sur la question de savoir si l'attaque était ou non un ransomware tel qu'il a été signalé, mais il a réitéré que le club avait informé le bureau chargé du suivi des cyberattaques, ce que les organisations sont tenues de faire si des données personnelles sont compromises lors d'un incident de sécurité des données.

Plus tôt cette année, le NCSC a averti que les clubs de football étaient particulièrement vulnérables aux internet-enabled skull ducks, y compris aux attaques de hijack sur les e-mails commerciaux. Cela est principalement dû à la grande quantité de blanchiment d'argent autour du sport et à l'habitude de transférer de grandes quantités d'argent à des moments prévisibles tels que les délais de transfert.

***Source :*** *https://bit.ly/33qoI4g*

## Les cybercriminels lancent une vague d'attaques sur des sites Wordpress vulnérables

27 novembre 2020

Lors d'un incident découvert récemment, un nouveau gang de cybercriminalité a exploité des sites WordPress vulnérables pour installer des magasins de commerce électronique frauduleux dans le but de réduire le classement et la réputation d'un site dans les moteurs de recherche.

Les attaquants ont eu accès au compte administrateur du site grâce à des attaques par force brute, après quoi ils ont écrasé le fichier d'index principal du site et ajouté du code malveillant.

Les chercheurs ont également découvert que des attaquants injectaient des fichiers PHP malveillants dans les sites WordPress pour assurer un flux constant de liens de spam SEO.

[…] Il n'est pas surprenant que des vulnérabilités non corrigées dans les logiciels de base de WordPress alimentent les ambitions malveillantes des cyberattaquants. Par conséquent, régler les problèmes de sécurité au bon moment et suivre les meilleures pratiques de cybersécurité est une réponse pour sécuriser les sites WordPress contre les cyberattaques.

***Source :*** *https://bit.ly/36hk4Ho*

# Evènements

## Evènements du mois

### CyberTech Africa

**22-24 Novembre 2020, Kigali, Rwanda**

https://bit.ly/3jwPopb

La Cybertech Africa a servi de lieu de rencontre pour les décideurs locaux et internationaux pour tout ce qui concerne la cybersécurité et l'innovation. L'événement a offert une plate-forme pour découvrir, discuter et analyser les défis, les solutions et les développements technologiques qui sont à la pointe de l'innovation et de la cybersécurité mondiales. Les sujets ont inclut la fintech, la confidentialité, l'IoT, les infrastructures critiques, la cyber-sensibilisation et bien plus encore ! Combinant l'écosystème local et l'expertise internationale, les orateurs ont englobé des hauts fonctionnaires et des dirigeants de l'industrie.


### Global Talent

**10 Novembre 2020, Online**

https://bit.ly/3oa9zvV

Ce panel virtuel s'est concentré sur l'optimisation des entreprises de services financiers pour faire face à l'évolution du milieu de travail du futur.

Cet événement s'est adressé en particulier aux leaders de la sécurité des services financiers.

Au cours de ce panel, des experts ont partagé leurs conseils, leurs expertises et leurs meilleures pratiques sur l'évolution du lieu de travail et de la main-d'œuvre du futur.

Un examen plus approfondi de la façon dont les paradigmes de collaboration émergents peuvent affecter les stratégies.

Une plongée en profondeur dans la confidentialité des données au-delà des frontières géographiques.


### Cybersecurity Leadership Summit 2020

**09-11 Novembre 2020, Online**

https://bit.ly/2VfWqoH

Avec 3 jours de contenu, plus de 60 conférenciers, 40 meilleures pratiques et des sessions interactives. Les participants avaient l'occasion idéale d'apprendre les dernières tendances et les défis auxquels leurs pairs sont confrontés. Parmi les sujets clés abordés lors de cet événement : la réponse aux incidents, la sécurité OT / IoT, la confidentialité, la gestion des risques et d'autres sujets issus des expériences quotidiennes des leaders de la cybersécurité.

## Evènements à venir

### Conférence internationale sur l'informatique avancée et l'ingénierie intelligente (ICACIE)

**28-29 Décembre 2020, UAE, Dubai**

https://bit.ly/3g0JdcZ

L'objectif principal de la Conférence internationale sur l'informatique avancée et l'ingénierie intelligente (ICACIE) est de discuter des difficultés liées à l'administration pratique de toutes les informations avancées produites dans les domaines de l'ingénierie intelligente et de l'informatique avancée.

Compte tenu de la vitesse à laquelle les progrès dans ces domaines se produisent, les jeunes universitaires et les chercheurs en début de carrière ont plus de difficulté que jamais à se tenir constamment informés. Cet événement s'efforce de les aider à se mettre à jour avec toutes les améliorations les plus modernes et les plus récentes.

| | |
|---|---|
| **Reference** | ANPT-2020-BV-11 |
| **Titre** | Bulletin de veille N°11 |
| **Date de version** | 30 Novembre 2020 |
| **Contact** | ssi@anpt.dz |