BULLETIN DE VEILLE N°11

ANPT-2021-BV-11

« For every lock, there is someone out there trying to pick it or break in »
-David Bernstein-

Novembre 2021

Alertes de sécurité

ZOOM

Zoom corrige des failles critiques dans ses produits

09-24 Novembre 2021

Zoom a publié des correctifs pour des vulnérabilités qui exposent les utilisateurs à des attaques par exécution de code à distance ou injection de commande.

La société a publié un bulletin de sécurité listant les vulnérabilités corrigées, parmi lesquelles on trouve trois problèmes de sécurité « à haut risque » comme CVE-2021-34417 (score CVSS de 7.9), qui est une faille d'exécution de commande à distance affectant plusieurs composants logiciels Zoom : Zoom On-Premise Meeting Connector Controller, Zoom On-Premise Meeting Connector MMR, Zoom On-Premise Recording Connector, Zoom On-Premise Virtual Room Connector.

Une autre vulnérabilité à haut risque, nommée CVE-2021-34422 (score CVSS de 7.9), est un bug de traversée de chemin affectant Keybase Client pour Windows.

L'entreprise a également publié des correctifs pour une faille à risque moyen (CVE-2021-34420) dans le programme d'installation de « Zoom Client for Meetings ».

Le logiciel Zoom ne dispose pas d'un mécanisme de mise à jour automatique. Les utilisateurs sont invités à vérifier et appliquer manuellement les mises à jour du logiciel dans le client Zoom.

Source : *https://bit.ly/3xzY5HG*

Intel

Une vulnérabilité grave dans certain processeur Intel

15 Novembre 2021

Des chercheurs ont découvert une vulnérabilité dans les processeurs Intel qui pourrait affecter les ordinateurs portables, les voitures et les systèmes embarqués. La faille (CVE-2021-0146) permet des modes de test ou de débogage sur plusieurs lignes de processeurs Intel, ce qui pourrait permettre à un utilisateur non autorisé disposant d'un accès physique d'obtenir des privilèges accrus sur le système.

Ce problème a été découvert dans les processeurs Pentium, Celeron et Atom des plateformes Apollo Lake, Gemini Lake et Gemini Lake Refresh, qui sont utilisés à la fois dans les appareils mobiles et les systèmes embarqués.

La menace, qui a reçu un score de 7,1, affecte une large gamme de netbooks ultra-mobiles et une base importante de systèmes IoT basés sur Intel, allant des appareils électroménagers et des systèmes de maison intelligente aux voitures et aux équipements médicaux.

Pour corriger la vulnérabilité découverte, installez les mises à jour du BIOS UEFI publiées par les fabricants finaux des équipements électroniques concernés (ordinateurs portables ou autres appareils).

Sources : https://bit.ly/3FUCbBX

Cisco

Une faille de gravité élevée affecte les pare-feu Cisco

22 Novembre 2021

Une vulnérabilité a été découverte dans les pare-feu de Cisco ASA (Adaptive Security Appliance) et Cisco FTD (Firepower Threat Defense) pourrait entraîner une interruption de l'accès à distance.

La faille, nommée CVE-2021-34704 et ayant un score de 8,6, peut être exploitée en envoyant des requêtes spécialement pour déclencher un dépassement de tampon (Buffer Overflow), le système touché s'arrête alors brusquement et redémarre et les employés qui travaillent à distance seront bloqués pour accéder au réseau interne de leur organisation.

Nikita Abramov, le chercheur de Positive Technologies qui a détecté le problème, a déclaré : "Si des pirates informatiques perturbent le fonctionnement de Cisco ASA et Cisco FTD, une entreprise se retrouvera sans pare-feu et sans accès à distance (VPN). Si l'attaque réussit, les employés ou partenaires distants ne pourront pas accéder au réseau interne de l'entreprise, et l'accès depuis l'extérieur sera restreint. En même temps, la défaillance du pare-feu réduira la protection de l'entreprise."

Un correctif a été créé pour cette faille et les utilisateurs sont invités à suivre les recommandations du fabricant décrites dans son avis de sécurité et à installer les mises à jour dès que possible.

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

Des correctifs urgente pour les commutateurs Catalyst

04 Novembre 2021

Cisco a publié des mises à jour de sécurité pour corriger des failles dans plusieurs équipements pouvant donner à un attaquant la possibilité de prendre le contrôle des systèmes concernés. La faille la plus critique, référencée CVE-2021-34795 et qui a un score de gravité de 10 sur 10, permet à un attaquant non authentifié de se connecter à distance avec un compte de débogage qui a un mot de passe codé en dur, via Telnet si le protocole est activé.

Les correctifs traitent aussi la vulnérabilité CVE-2021-40119 qui touche la Cisco Policy Suite, outil de gestion. Un attaquant distant non authentifié pourrait se connecter à des systèmes non patchés en tant qu'utilisateur root (administrateur).

Sources : *https://bit.ly/3I2Q82B*

AMD

AMD corrige des dizaines de problèmes de sécurité dans les pilotes graphiques de Windows 10

11 Novembre 2021

AMD a corrigé une longue liste de failles de sécurité trouvées dans son pilote graphique pour les appareils Windows 10, permettant aux attaquants d'exécuter du code arbitraire, d'élever leurs privilèges et de provoquer des dénis de service et des divulgations d'informations.

L'impact potentiel et la gravité des failles varient, AMD ayant étiqueté dix-huit (18) bugs comme étant de haute gravité, parmi lesquelles nous trouvons CVE-2020-12902 qui est une vulnérabilité d'escalade de privilèges et CVE-2020-12893 qui est un buffer overflow de pile dans le pilote graphique AMD.

Une liste complète des vulnérabilités trouvées dans le pilote graphique AMD pour Windows 10 et leur description est disponible dans l'avis de sécurité de l'entreprise.

Sources : https://bit.ly/3D4hhib

Linux

Une vulnérabilité "dangereuse" touche Linux

04 Novembre 2021

Des chercheurs attirent l'attention sur un problème de sécurité récemment découvert dans un module du noyau livré avec toutes les principales distributions de Linux, en prévenant que des attaquants distants peuvent exploiter le bug pour prendre le contrôle complet d'un système vulnérable.

La vulnérabilité (CVE-2021-43267) est un débordement de la mémoire tas dans le module TIPC (Transparent Inter-Process Communication) qui est livré avec le noyau Linux pour permettre aux nœuds d'un cluster de communiquer entre eux de manière tolérante aux pannes.

"La vulnérabilité peut être exploitée localement ou à distance au sein d'un réseau pour obtenir les privilèges du noyau, permettant à un attaquant de compromettre l'ensemble du système", selon un avertissement de Max Van Amerongen de SentinelOne, le chercheur en sécurité qui a découvert - et aidé à corriger- la vulnérabilité.

"Comme cette vulnérabilité a été découverte moins d'un an après son introduction dans la base de code, les utilisateurs de TIPC doivent s'assurer que la version de leur noyau Linux n'est pas comprise entre 5.10-rc1 et 5.15", a-t-il ajouté.

Source : https://bit.ly/3I4u0Fi

Microsoft

Une vulnérabilité Zero-Day avec un exploit publiquement disponible !

23 Novembre 2021

Un chercheur en sécurité a publiquement divulgué un exploit pour une nouvelle vulnérabilité zero-day. Windows d'élévation de privilèges locaux qui peut être exploitée par des acteurs de la menace pour obtenir des privilèges d'administrateur dans Windows 10, Windows 11 et Windows Server. La vulnérabilité peut être exploitée par des acteurs de la menace pour élever leurs privilèges afin d'effectuer de multiples activités malveillantes.

Le chercheur en sécurité Abdelhamid Naceri a découvert la faille zero-day en analysant un correctif de sécurité publié par Microsoft dans le cadre du Patch Tuesday de novembre pour une autre vulnérabilité d'élévation de privilèges de Windows Installer, suivie sous le nom de CVE-2021-41379, que le chercheur a signalée à Microsoft.

"Cette variante a été découverte lors de l'analyse du patch CVE-2021-41379. Le bug n'a pas été corrigé correctement", écrit l'expert.

En attendant que cette vulnérabilité soit corrigée, Cisco Talos ont publié les recommandations à suivre pour se protéger des éventuelles attaques.

Source : https://bit.ly/2ZywYjX

Microsoft corrige une faille XSS dans Exchange Server

16 Novembre 2021

Microsoft a corrigé une vulnérabilité de type cross-site scripting dans Exchange Server qui pourrait causer une usurpation d'identité.

Repérée sous le nom de CVE-2021-41349, la faille de gravité moyenne (score CVSS 6,5) a une faible complexité d'attaque, selon Microsoft,

"Comme il s'agissait d'un simple XSS, un attaquant aurait pu manipuler le DOM et l'utiliser pour lire/envoyer des courriels, faire du phishing, effectuer des actions de changement d'état dans l'application, etc. », a déclaré le chercheur en sécurité Rahul Maini.

Microsoft a publié cinq mises à jour applicables à Exchange Server 2013, 2016 et 2019 qui traitent de la vulnérabilité.

Source : https://bit.ly/3E6ZLeg

Actualité

Guess who's back

Novembre 2021

Malgré les efforts déployés par les chercheurs pour détecter et éliminer les malwares, il ne semble pas que les acteurs de la menace soient prêts à s'arrêter. De nouvelles variantes du malware déjà identifié apparaissent régulièrement. Pendant ce mois seulement, plusieurs variantes de malwares existants ont été observées, en voilà quelques-unes :

AbstractEmu :

Récemment, le Lookout Threat Lab a découvert la première campagne de malware d'enracinement depuis cinq ans. Baptisé AbstractEmu en raison de son utilisation de l'extraction de code et des contrôles anti-émulation pour éviter la détection, le malware a été trouvé sur Google Play et d'autres magasins d'applications tiers importants tels que Amazon Appstore et Samsung Galaxy Store.

AbstractEmu s'est déguisé en un certain nombre d'applications différentes, y compris des applications utilitaires, comme des gestionnaires de mots de passe, et des outils système comme des lanceurs d'applications ou des économiseurs de données. En dissimulant ses intentions malveillantes derrière des applications apparemment inoffensives, l'acteur de la menace a pu inciter des utilisateurs peu méfiants à télécharger le malware.

Les chercheurs de Lookout ont trouvé un total de 19 applications liées au malware, dont 7 contenaient des fonctionnalités d'enracinement. Une des applications trouvées sur Google Play était confirmée d'avoir été téléchargée plus de 10.000 fois.

Lookout a informé Google et les applications ont été rapidement supprimées.

Emotet :

Des chercheurs ont découvert que le cheval de Troie TrickBot, l'un des systèmes de diffusion de logiciels malveillants les plus prolifiques et les plus nuisibles des botnets, semble faire un retour en force après près d'un an d'inactivité. Une équipe de chercheurs de Cryptolaemus, G DATA et AdvIntel ont récemment observés que le trojan TrickBot lançait ce qui semble être un nouveau loader pour le célèbre malware Emotet.

Emotet a commencé sa vie en tant que cheval de Troie bancaire en 2014 et a continuellement évolué pour devenir un mécanisme de diffusion de menaces à service complet. La dernière fois qu'Emotet a été vu en volume, il atteignait 100 000 boîtes aux lettres cibles par jour pour diffuser TrickBot, Qakbot et Zloader en décembre 2020. Il semble maintenant qu'il ait refait surface en utilisant son partenaire habituel TrickBot.

Les intentions réelles du malware n'étant pas encore claires, les organisations qui souhaitent se prémunir contre cette menace peuvent déjà se concentrer sur la formation de leur personnel aux dangers des menaces par courrier électronique et sur le renforcement de la surveillance du réseau, étant donné qu'Emotet propage les infections principalement par le biais de campagnes de phishing.

Joker :

Le malware Joker qui a été découvert la première fois en 2017 est une menace sophistiquée et dangereuse pour les utilisateurs d'Android. Cette famille de malwares effectue principalement des fraudes de facturation et vole des SMS et des informations sur les appareils. De plus, elle télécharge des charges utiles malveillantes. Les développeurs du malware utilisent régulièrement des techniques mises à jour, telles que des charges utiles à plusieurs étapes, pour éviter la détection.

Une nouvelle série de variantes du malware Joker a été découverte se propageant via le Play Store par Cyble Research Labs. Ces variantes ont utilisé des techniques sophistiquées pour éviter le moteur de détection des malwares de Google.

Pour diffuser ces nouvelles variantes, les attaquants ont créé des applications malveillantes se faisant passer pour des applications légitimes courantes. Dans les attaques récentes, une variante du Joker a été observée exploitant la popularité de Squid Game pour attirer des victimes peu méfiantes. Dans un autre cas, l'application malveillante s'est fait passer pour une application officielle de clignotement de LED qui utilise des LEDs comme notifications pour les appels et les SMS entrants. Dans cette dernière, 18 autorisations sont demandées à Android, dont trois sont utilisées par le malware. En conséquence, il est recommandé d'éviter les applications provenant de sources tierces non fiables et de surveiller le comportement des applications installées pour rester protégé.

Lazarus :

Lazarus, un groupe de pirates sponsorisé par l'État nord-coréen, connu pour ses attaques visant les chercheurs en sécurité, est revenu en force, cette fois avec une version piratée de l'application populaire de rétro-ingénierie IDA Pro.

Bien qu'il n'ait jamais été déterminé quel était le but ultime de ces attaques, il semble que ce soit le vol de vulnérabilités et exploits de sécurité non divulgués que le groupe de pirates pourrait utiliser dans ses propres attaques. Les chercheurs en cybersécurité utilisent généralement IDA pour examiner les failles et les logiciels malveillants dans les logiciels légitimes afin de déterminer les comportements malveillants qu'ils présentent. Comme il s'agit d'un logiciel coûteux, certain chercheurs tournent parfois vers sa version piratée. Les versions piratées comportent le risque de contenir des exécutables malveillants, ce qui est le cas de la version malveillante d'IDA Pro 7.5.

Le programme d'installation d'IDA a été modifié pour inclure deux DLL malveillantes nommées idahelp.dll et win_fw.dll qui seront exécutées lors de l'installation du programme.

Bien qu'il n'ait jamais été déterminé quel était le but ultime de ces attaques, il s'agissait probablement de voler des vulnérabilités

de sécurité non divulguées et des exploits que le groupe de pirates pourrait utiliser dans ses propres attaques.

Du cinéma au monde réel : L'authentification biométrique par empreinte est contournée

19 Novembre 2021

Dans les films, on voit souvent des personnes se servir de ruban adhésif pour décoller une empreinte digitale d'une surface et l'appliquer sur un scanner d'empreintes digitales. Cela semble fonctionner dans les films mais êtes-vous déjà demandé si cela fonctionne dans la réalité ?

En fait, le ruban adhésif ne fonctionne peut-être pas, mais l'équipe de Kraken Security Labs a réussi à trouver un moyen permettant de contourner l'authentification par empreinte digitale. Selon ces derniers, il existe un moyen de cloner des empreintes digitales à l'aide de matériaux peu coûteux, sans qu'aucun outil haut de gamme n'intervienne à aucune étape du processus, une photo de l'empreinte digitale, une imprimante et de la colle, c'est tout ce dont ils avaient besoin pour créer un clone de l'empreinte.

Comme l'équipe l'a démontré dans une vidéo, voler l'empreinte digitale consiste à la photographier avec n'importe quel smartphone moderne, puis à générer le négatif sur un logiciel de manipulation de photos. Pour l'étape d'impression, toute imprimante laser acceptant les feuilles en acétate conviendrait pour l'attaque. L'acétate est généralement utilisé pour les cartes,

Les pochoirs et les superpositions, mais il est idéal dans ce cas car l'imprimante laser peut le graver. Une fois l'impression terminée, l'empreinte peut être assemblée en appliquant de la colle à bois sur l'empreinte et en la laissant sécher.

Grâce à des tests, l'équipe de Kraken a constaté que l'empreinte digitale obtenue pouvait tromper les capteurs d'empreintes digitales les plus modernes, comme celui utilisé dans le dernier MacBook Pro.

Les résultats de laboratoire Kraken ne signifient pas que la fin des empreintes digitales est proche, mais ils constituent un bon rappel de la raison pour laquelle les gens ne devraient pas les considérer comme une couche unique de protection de leurs comptes, ce qui nous rappelle l'importance de l'authentification multifactorielle.

Source : *https://bit.ly/3FT4eBW*

CISA : Nouveau guide de réponse aux incidents et aux vulnérabilités de cybersécurité

16 Novembre 2021

CISA a publié le guide de réponse aux incidents de cybersécurité et aux vulnérabilités du gouvernement fédéral. Ce manuel fournis aux agences fédérales civiles de l'exécutif (FCEB) des procédures opérationnelles pour planifier et mener des activités de réponse aux incidents de cybersécurité et aux vulnérabilités. Il contient également des arbres de décision illustrés et détaille chaque étape de la réponse aux incidents et aux vulnérabilités.

Bien que le CISA ait créé les manuels pour les agences FCEB, Il est recommandé que les autres entités de l'examiner afin de référencer et comparer leurs propres pratiques.

Source : *https://bit.ly/3FUudc1*

Cloud… soyons prêts !

Choisir un seul cloud ou opter pour le multi-cloud ?

La base pour choisir le bon fournisseur de cloud peut varier d'une organisation à l'autre, selon ses propres exigences commerciales et ses propres besoins en matière de cloud. Nous vous présentons ci-dessous certains points clés aidant à évaluer les différents fournisseurs :

1. Comprendre les besoins de l'entreprise : Avant tout, il est primordial de comprendre en détails, les exigences et les besoins de l'entreprise puis chercher la liste des fournisseurs qui réponde à ces besoins.
2. Coût du fournisseur de services en nuage : Il faut choisir un fournisseur avec des tarifs convenables au budget de l'entreprise
3. Sécurité des données : Avant d'intégrer un service de cloud computing, Il est nécessaire de comprendre la politique de sécurité des données du fournisseur Cloud et définir le niveau de sécurité qui doit être garantie.
4. Avancées technologiques Vérifiez si le fournisseur de services en nuage vous offre la dernière technologie ou la technologie compatible avec les besoins de votre entreprise
5. Support : Avec l'énorme quantité de données sur le cloud, il peut y avoir de nombreux cas où vous pouvez avoir besoin de l'assistance des fournisseurs de cloud pour tout problème. Il est préférable d'avoir un fournisseur qui offre une assistance 24 heures sur 24, 7 jours sur 7.
6. Fiabilité : il est conseillé de vérifier la fiabilité du fournisseur en fonction des tendances passées, et comment il peut gérer les temps d'arrêt imprévus et la récupération des données en cas d'incident.

7. Certifications et normes : Les fournisseurs qui se conforment aux normes mondiales reconnues et aux cadres de qualité démontrent leur adhésion aux meilleures pratiques et normes du secteur. Si les normes ne déterminent pas forcément le choix du fournisseur de services, elles peuvent être très utiles pour présélectionner les fournisseurs potentiels.

Les points ci-dessus constituent une bonne base pour construire un cadre analytique solide à utiliser pour choisir le fournisseur approprié. Il est conseillé de penser à long terme pour éviter les éventuels blocages futurs.

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

Bon à savoir !

Votre hygiène de cybersécurité est pire que ce que vous pensez !

Tout comme vous avez des habitudes d'hygiène personnelle pour préserver votre propre santé, les bonnes pratiques de cyber-hygiène contribuent à protéger la santé du réseau et des actifs de votre organisation. Certaines entreprises les ignorent en pensant qu'elles sont facultatives, et d'autres se contentent d'appliquer une partie en pensant que c'est suffisant.

Sevco Security a publié un rapport qui explore la marge entre les perceptions et les réalités en termes d'hygiène de la sécurité et de gestion des actifs. Ils ont découvert qu'en moyenne, les organisations découvrent 20 à 30% de dispositifs précédemment inconnus une fois que les diverses sources d'inventaire et d'audit ont été analysées et réconciliées.

Cette marge représente un vrai problème car comme a déclaré J.J. Guy, PDG de Sevco "il est impossible de sécuriser ce que vous ne pouvez pas voir". Et si elles ne sont pas corrigées, ces lacunes peuvent se transformer en vulnérabilités sérieuses et en zones de risque accru pour la sécurité.

De ce fait, pour assurer une meilleure gestion des actifs, il est recommandé de commencer par définir clairement le responsable de l'inventaire des biens, car de nombreux problèmes liés à l'inventaire des biens découlent de la propriété cloisonnée d'outils permettant d'obtenir des données d'inventaire. De plus, il est conseillé de modifier les processus d'inventaire des actifs pour qu'ils soient continus et non pas périodique. Et finalement, il ne faut garder en tête qu'une mauvaise compréhension de l'inventaire des actifs peut ruiner les efforts qui peuvent être remarquables, comme un programme de gestion des vulnérabilités.

***Sources** : https://bit.ly/3E6YxzY*

Evènement

Evènements du mois

14ème édition de la conférence annuelle du SECITC

25-26 Novembre 2021

Online

https://bit.ly/3p3W3vM

La 14ème conférence annuelle du SECITC a réuni des chercheurs en sécurité informatique, des cryptographes, des représentants de l'industrie et des étudiants diplômés intéressés par la sécurité et la confidentialité des informations. L'un de ses principaux objectifs était de mettre en contact des chercheurs en sécurité et en protection de la vie privée ainsi que des professionnels de différentes communautés et de fournir un forum permettant les échanges informels nécessaires à l'émergence de nouvelles collaborations scientifiques et industrielles.

Evènements à venir

2ème Edition du Sheo-tech Days

17 au 19 Décembre 2021

Online

https://bit.ly/3FZr3nl

Les Sheo-tech Days est un événement en ligne, annuel et gratuit, de sensibilisation à la sécurité informatique, la protection des données et le cyber-harcèlement, porté par la société Sheo Technology et ses partenaires. Les conférences et tables rondes seront en ligne et porteront sur des sujets liés aux environnements Active Directory, Microsoft 365, la sensibilisation des utilisateurs et des dirigeants, le cyber harcèlement, le cloud Azure et AWS, le développement sécurisé, la conformité RGPD, la gestion d'un cyber attaque et d'autres encore.

Référence	ANPT-2021-BV-11
Titre	Bulletin de veille N°11
Date de version	30 Novembre 2021
Contact	ssi@anpt.dz