BULLETIN DE VEILLE N°12

ANPT-2021-BV-12

« If you think you know-it-all about cybersecurity, this discipline was probably ill-explained to you »

-Srephane Nappo-

Décembre 2021

Alertes de sécurité

Wordpress

Le plugin populaire SEO est affecté par deux vulnérabilités critiques

22 Décembre 2021

Deux failles de sécurité dans le populaire plugin WordPress "All in One" SEO ont exposé plus de 3 millions de sites web à des attaques de prise de contrôle.

Le premier bug critique est une escalade de privilèges authentifiés (CVE-2021-25036) et le second est une injection SQL authentifiée de haute gravité (CVE-2021-25037).

Comme l'a révélé Marc Montpas, le chercheur en sécurité qui a découvert les failles, l'élévation des privilèges en abusant de CVE-2021-25036 est une tâche facile en "changeant un seul caractère en majuscule" pour contourner toutes les vérifications de privilèges mises en œuvre.

"C'est particulièrement inquiétant car certains des points de terminaison du plugin sont assez sensibles. Par exemple, le point de terminaison aioseo/v1/htaccess peut réécrire le fichier .htaccess d'un site avec un contenu arbitraire", explique Montpas.

"Un attaquant pourrait abuser de cette fonctionnalité pour cacher des backdoors .htaccess et exécuter du code malveillant sur le serveur."

Les administrateurs de WordPress qui utilisent encore les versions d'All In One SEO qui n'ont pas encore installé le correctif 4.1.5.3 sont invités à le faire immédiatement.

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

Apache

LOG4J : La vulnérabilité de l'année

17 Décembre 2021

Une vulnérabilité a été trouvée dans apache log4j et son PoC a été rendu publique.

Étant donné que Log4j est intégré dans la majorité des applications Java, qui est utilisé dans des dizaines de technologies, Log4Shell s'est rapidement transformé en un cauchemar pour les entreprises et les gouvernements du monde entier.

Les vulnérabilités en question sont les suivantes :

- CVE-2021-44228 : Une faille d'exécution de code à distance (RCE) sans authentification, permettant une prise de contrôle complète du système. Classée critique, avec un score de 10 sur 10. Un correctif pour Log4Shell a été déployé dans la version 2.15.0, mais il a été jugé incomplet.
- CVE-2021-45046 : Une faille de déni de service qui résulte d'une correction incomplète de la CVE-2021-44228.
- CVE-2021-45105 : Il a été découvert par la suite que Log4j 2.16.0 aussi est vulnérable à une faille DoS d'une sévérité élevée. Apache a depuis publié une version 2.17.0 de Log4j corrigeant la CVE.

Pour remédier à ces vulnérabilités le centre gouvernemental de veille et de réponse aux attaques informatiques français (CERT-FR) recommande :

Aux utilisateurs d'applications ou de logiciels basés sur la technologie Java/J2EE :

- De conserver les journaux au moins depuis le 1er décembre 2021 à des fins d'analyse ultérieure ;
- De préparer des mesures de préservation en cas d'incident majeur, notamment par la mise hors ligne de sauvegardes à jour ;
- De filtrer et de journaliser les flux sortants des serveurs pour les limiter aux seuls flux autorisés vers des services de confiance ;
- De prendre contact avec le développeur ou l'éditeur pour vérifier s'ils sont exposés à cette vulnérabilité et si un correctif est disponible.

Aux développeurs/éditeurs :

- D'inventorier les solutions affectées par les vulnérabilités ;
- D'informer les utilisateurs et clients de leurs statuts et des actions en cours ;
- De corriger les solutions en utilisant la version 2.17.0 pour java 8 ou la version 2.12.3 (à venir) pour java 7 ;
- De fournir une nouvelle version de leurs solutions dans les plus brefs délais.

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

DELL

Des mises à jour du BIOS de Dell empêchent les ordinateurs de démarrer

21 Décembre 2021

Des mises à jour récentes du BIOS de Dell étaient à l'origine de graves problèmes de démarrage sur plusieurs modèles d'ordinateurs portables et de bureau.

Les modèles concernés sont les ordinateurs portables Dell Latitude (5320 et 5520), ainsi que les ordinateurs de bureau Dell Inspiron 5680 et Alienware Aurora R8.

Bien que les systèmes concernés s'allument, les utilisateurs affirment que les lumières et les écrans périphériques ne s'allument pas. Lorsqu'ils démarrent, ils passent directement à un écran bleu et s'éteignent à nouveau.

La solution de facilité, jusqu'à ce que Dell publie une mise à jour pour corriger les bogues conduisant aux problèmes de démarrage, consiste à rétrograder à une version antérieure du micrologiciel.

Il est possible de consulter les conseils officiels de Dell sur la façon de mettre à niveau le BIOS du système vers une version antérieur.

Source : *https://bit.ly/3144dwa*

Python

Des bibliothèques PyPI malicieuses téléchargés plus de 10,000 fois

13 Décembre 2021

Le registre du Python Package Index (PyPI) a supprimé trois bibliothèques Python malveillantes visant à exfiltrer des variables d'environnement et à déposer des chevaux de Troie sur les machines infectées.

Les bibliothèques concernées (aws-login0tool, dpp-client et dpp-client1234) ont été téléchargées et copiés près de 15 000 fois.

Le paquet aws-login0tool cible les machines Windows et télécharge un exécutable malveillant, normal.exe, depuis le domaine tryg[.]ga, qui a été identifié comme un cheval de Troie par 38 % des moteurs antivirus de VirusTotal

Les deux autres ciblent les systèmes Linux et s'intéressent aux variables d'environnement, au listing des répertoires, et exfiltrent ces informations vers le domaine pt.traktrain[.]com.

Ces paquages tentent d'espionner certains répertoires, dont /mnt/mesos, ce qui indique que le malware recherche spécifiquement des fichiers liés à Apache Mesos, un produit open source de gestion de clusters.

Source : *https://bit.ly/32Jg17m*

Microsoft

PoC publique pour deux vulnérabilités d'Active Directory

21 Décembre 2021

Microsoft alerte sur deux failles du contrôleur de domaine Active Directory après la publication des preuves de concept (PoC).

Les vulnérabilités identifiées comme CVE-2021-42287 et CVE-2021-42278, qui ont tous deux été corrigés dans la version du Patch Tuesday de novembre 2021, sont des failles d'escalade de privilèges qui donnent aux attaquants un accès direct aux privilèges d'administrateur ce qui mène à la prise de contrôle du domaine.

"En combinant ces deux vulnérabilités, un attaquant peut créer un chemin direct vers un utilisateur administrateur du domaine dans un environnement Active Directory qui n'a pas appliqué ces nouvelles mises à jour", selon l'alerte de sécurité. "Cette attaque par escalade permet aux attaquants d'élever facilement leurs privilèges à ceux d'un administrateur de domaine une fois qu'ils ont compromis un utilisateur ordinaire du domaine."

Les clients de Microsoft sont invités à appliquer les correctifs immédiatement. De plus, L'équipe de recherche de Microsoft a publié des conseils détaillés sur la détection des signes d'exploitation.

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

Des vulnérabilités non corrigées dans le logiciel Microsoft Teams !

22 Décembre 2021

Quatre vulnérabilités ont été découvertes dans la plateforme Teams. Sur les quatre vulnérabilités, Microsoft n'en aurait corrigé qu'une seule qui entraîne la fuite de l'adresse IP des appareils Android. Microsoft précisant qu'un correctif pour la faille de déni de service (DoS) sera envisagé dans une future version du produit.

La principale faille est une vulnérabilité qui pourrait être exploitée pour glaner des informations sur le réseau local de Microsoft.

La seconde est un bug d'usurpation d'identité dans lequel la cible du lien de prévisualisation peut être modifiée pour pointer vers n'importe quelle URL malveillante.

La vulnérabilité DoS, qui affecte la version Android de Teams, peut faire planter l'application simplement en envoyant un message avec un aperçu de lien spécialement conçu.

Le dernier problème concerne une fuite d'adresse IP, qui affecte également l'application Android. En interceptant les messages qui incluent un aperçu de lien pour faire pointer l'URL de la vignette vers un domaine non-Microsoft, Positive Security a déclaré qu'il est possible d'accéder à l'adresse IP d'un utilisateur et aux données de l'agent utilisateur.

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

Actualité

2021 TOP HACKS

2021 a été une saison ouverte par les brèches, les ransomwares, l'espionnage et les violations de données. Nous listons dans ce qui suit ceux qui ont le plus marqué cette année :

Kaseya

L'une des attaques les plus mémorables de l'année 2021 : Début Juillet, des pirates associés au gang de ransomware REvil, ont exploité une faille dans l'outil Virtual System Administrator de Kaseya, et ont pu infecter jusqu'à 1 500 organisations dans le monde avec un ransomware. REvil a fixé des rançons d'environ 45 000 dollars pour de nombreuses victimes en aval et jusqu'à 5 millions de dollars pour les fournisseurs de services gérés eux-mêmes. Le gang a également proposé de publier un outil de décryptage universel pour environ 70 millions de dollars mais il a ensuite disparu, laissant tout le monde dans l'ignorance. Fin Juillet, Kaseya a acquis un décrypteur universel et a commencé à le distribuer à ses clients.

Pegasus

Le développeur israélien de logiciels espions NSO Group est devenu de plus en plus le visage de l'industrie de la surveillance ciblée. La plateforme de communication WhatsApp a poursuivi NSO en 2019 et Apple lui a emboîté le pas cette année en novembre, après une série de révélations selon lesquelles NSO a créé des outils pour infecter des cibles iOS avec son logiciel espion phare Pegasus en exploitant des failles dans la plateforme de communication iMessage d'Apple. En Juillet, un groupe international de chercheurs et de journalistes d'Amnesty International, de Forbidden Stories et de plus d'une douzaine d'autres organisations a publié des preuves montrant qu'un certain nombre de gouvernements dans le monde pourraient être des clients de NSO. Les chercheurs ont étudié une liste divulguée de 50 000 numéros de téléphone associés à des activistes, des journalistes, des cadres et des politiciens qui étaient tous des cibles potentielles de surveillance. NSO Group a réfuté ces affirmations.

Microsoft Exchange

Le groupe de pirates connu sous le nom de Hafnium, ont exploité des vulnérabilités dans le logiciel Exchange Server de Microsoft, compromettant ainsi les messageries électroniques de leurs cibles. Les attaques ont touché des dizaines de milliers d'entités à travers les États-Unis à partir de Janvier et avec une intensité particulière dans les premiers jours de Mars. Les piratages ont touché un large éventail de victimes, notamment des petites entreprises et des administrations. La campagne a également touché un nombre important d'organisations en dehors des États-Unis, comme le Parlement norvégien et l'Autorité bancaire européenne. Microsoft a publié des correctifs d'urgence le 2 Mars pour remédier aux vulnérabilités, mais la vague de piratage était déjà en marche.

Log4Shell (To be Continued …)

Le Jeudi, 09 Décembre, un exploit PoC pour la vulnérabilité critique Log4j a été publié sur GitHub. Il s'est suivi par une divulgation de la vulnérabilité et une activité de balayage massif de la part des attaquants ciblant les serveurs vulnérables.

Les attaquants sont en train d'exploiter cette vulnérabilité afin de créer un reverse shell, qui leur permet de contrôler à distance le serveur ciblé, ou faire du serveur ciblé une partie d'un botnet

A l'heure actuelle, plusieurs attaques ont été réussites, comme par exemple des gangs de ransomware qui ont verrouillé des serveurs Minecraft, des groupes de pirates qui tentant de miner des bitcoins ou alors l'attaque qui a ciblé le ministère belge de la défense.

Bien que la vulnérabilité ait été portée à l'attention du public pour la première fois le 10 Décembre 2021, les gens continuent d'identifier de nouvelles façons de causer des dommages grâce à ce mécanisme.

Sa difficulté réside dans le fait de ne pas savoir si Log4j est utilisé dans un système logiciel donné, car il est souvent intégré à d'autres logiciels. Ainsi que la diversité des utilisations de Log4j est qu'il n'existe pas de solution unique pour le corriger. Selon la façon dont Log4j a été intégré dans un système donné, la correction nécessitera différentes approches. Elle peut nécessiter une mise à jour complète du système, ou le passage à une nouvelle version du logiciel, ou encore la suppression manuelle du code vulnérable pour ceux qui ne peuvent pas mettre à jour le logiciel, ce qui signifie que ce problème nécessitera des semaines ou même des mois afin d'être résolu.

***Source** : https://bit.ly/3FyZ7Hq*

DarkWatchman : Un nouveau malware qui se cache dans le registre de Windows

19 Décembre 2021

Un nouveau logiciel malveillant baptisé "DarkWatchman" a fait son apparition. Il s'agit d'un cheval de Troie d'accès à distance (RAT) JavaScript associé à un keylogger C#.

Selon un rapport technique des chercheurs de Prevailion, les acteurs de menace distribuent le malware par le biais d'e-mails de phishing contenant des pièces jointes ZIP malveillantes qui comporte un exécutable utilisant une icône pour se faire passer pour un document texte. Cet exécutable est une archive WinRAR auto-installée qui installera le RAT et le keylogger.

S'il est ouvert, l'utilisateur voit apparaître un message popup indiquant "Format inconnu", mais en réalité, les charges utiles ont été installées en arrière-plan.

L'aspect fascinant de DarkWatchman est son utilisation du mécanisme de stockage sans fichier du Registre Windows pour le keylogger : "Le keylogger est distribué sous forme de code source C# obscurci qui est traité et stocké dans le registre comme une commande PowerShell codée en Base64. Lorsque le RAT est lancé, il exécute ce script PowerShell qui, à son tour, compile le keylogger (à l'aide de CSC) et l'exécute", expliquent les chercheurs de Prevailion Matt Stafford et Sherman Smith.

"Le keylogger lui-même ne communique pas avec le C2 et n'écrit pas sur le disque. Au lieu de cela, il écrit son keylog dans une clé de registre qu'il utilise comme tampon. Pendant son fonctionnement, le RAT gratte et efface ce tampon avant de transmettre les frappes enregistrées au serveur C2."

En ce qui concerne la communication et l'infrastructure C2, les acteurs de DarkWatchman utilisent des DGA (algorithmes de génération de domaines) avec une liste d'amorçage de 10 éléments pour générer jusqu'à 500 domaines par jour.

Cela leur confère une excellente résilience opérationnelle et, en même temps, rend la surveillance et l'analyse des communications très difficiles.

***Source** : https://bit.ly/3EEl0DD*

Diffusion du malware StrongPity via des installeurs de Notepad++

09 Décembre 2021

Le groupe de pirates StrongPity est en train de faire circuler des installateurs Notepad++ qui infectent les cibles avec des logiciels malveillants.

Lors de l'exécution du programme d'installation, le fichier crée un dossier nommé "Windows Data" sous C:\ProgramData\Microsoft, et dépose les trois fichiers suivants : npp.8.1.7.Installer.x64.exe, winpickr.exe et ntuis32.exe.

L'installation de l'éditeur de code se poursuit comme prévu, et la victime ne voit rien d'anormal.

À la fin de l'installation, un nouveau service nommé "PickerSrv" est créé, établissant la persistance du malware via l'exécution au démarrage. Ce service exécute 'ntuis32.exe', qui est le composant keylogger du malware.

Le keylogger enregistre toutes les frappes de l'utilisateur et les sauvegarde dans des fichiers système cachés créés dans le dossier 'C:\ProgramData\Microsoft\WindowsData'. Le malware a également la capacité de voler des fichiers et d'autres données du système.

Ce dossier est vérifié en permanence par "winpickr.exe" et lorsqu'un nouveau fichier journal est détecté, le composant établit une connexion C2 pour télécharger les données volées vers les attaquants. Une fois le transfert terminé, le journal original est supprimé pour effacer les traces de cette activité.

C'est pour cela qu'il est toujours recommandé d'installer les applications des sites Web officiels associés.

***Source** : https://bit.ly/32CgYP0*

Bon à savoir !

Comment les organisations doivent gérer la réponse à Log4Shell ?

Le problème de Log4j peut avoir des conséquences graves pour de nombreuses organisations. La gestion de ce risque nécessite un leadership fort, les cadres supérieurs travaillant avec les équipes techniques pour comprendre d'abord l'exposition de leur organisation, puis pour prendre les mesures appropriées.

Selon le NCSC (National Cyber Security Center), les organisations de taille moyenne à grande disposant d'équipes informatiques dédiées devraient se poser les questions suivantes :

1. Qui dirige notre réponse ? : Log4shell est un incident critique qui nécessite la mise en place d'une équipe spéciale. Il devrait y avoir une personne désignée pour diriger la réponse de l'organisation.
2. Quel est notre plan ? : Actuellement, la plupart des organisations répondent à des logiciels jugés vulnérables ou à des cyber-attaques. On assistera probablement à une migration vers une approche plus méthodique qui permettra d'abord d'identifier comment l'organisation est affectée, puis de rectifier les problèmes constatés.
3. Comment saurons-nous si nous sommes attaqués et pourrons-nous réagir ? : Vos équipes sauront-elles si votre organisation est visée, et seront-elles prêtes à réagir dans ce cas ?
4. Quel pourcentage de visibilité de nos logiciels/serveurs avons-nous ? : Les équipes essaient de trouver des instances de logiciels et de Log4j lui-même. Cette tâche sera plus facile sur les actifs gérés par l'entreprise, mais moins sur les actifs non gérés.

5. Comment abordons-nous la question de l'informatique fantôme/des applications ? : En plus de réparer les biens gérés par l'entreprise, les équipes doivent réfléchir à la manière dont elles vont découvrir les choses qui ont pu passer à travers les mailles du filet et qui ne sont pas gérées de manière centralisée (souvent appelées "shadow IT").
6. Savons-nous si les principaux fournisseurs se couvrent eux-mêmes ? : Si votre organisation dépend de fournisseurs particulièrement importants, vous devez avoir une conversation ouverte et honnête avec eux sur la situation.
7. Quelqu'un dans notre organisation développe-t-il du code Java ? Quel est leur plan pour savoir si nous sommes affectés ? : Les organisations peuvent produire du code Java pour un usage interne ou comme produit. Les développeurs Java peuvent avoir utilisé Log4j, il est donc important de s'assurer que tout logiciel écrit n'est pas vulnérable.
8. Comment les gens nous signaleront ils les problèmes qu'ils trouvent ? : De nombreux chercheurs en cybersécurité essaient de détecter les logiciels vulnérables. S'ils trouvent quelque chose sur votre domaine, peuvent-ils vous contacter facilement (par exemple, via un processus de divulgation des vulnérabilités) ?
9. Quand avons-nous vérifié pour la dernière fois nos plans de continuité des activités (PCA) et notre réponse aux crises ? : Vérifiez les processus de bout en bout de votre organisation en matière de PCA et de réponse aux crises afin de minimiser l'impact réel sur l'organisation en cas d'attaque réussie.
10. Comment empêchons-nous les équipes de s'épuiser ? : La résolution de ce problème peut prendre des semaines, voire des mois pour les grandes organisations. La combinaison d'une situation en constante évolution (et de la possibilité d'une attaque) peut prendre des semaines, voire des mois pour les grandes organisations.

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

Evènements

Evènement du mois

Act now on Log4Shell Vulnerability

20 Décembre 2021

Online

Ce Webinaire a été organisé pour parler de la vulnérabilité Log4j. Au cours de la session, CSO de Sumo Logic George Gerchow et Roland Palmer, VP du centre des opérations mondiales ont partagé :

- Les dernières informations sur la vulnérabilité d'Apache Log4j/Log4Shell.
- Comment déterminer si une organisation est touchée.
- Comment la plateforme et les solutions Sumo Logic, natives du cloud, atténuent cette vulnérabilité.

Evènement à venir

Bsides Alger

08 au 09 Janvier 2022

L'ESI (Ecole Nationale Supérieure d'Informatique), Oued Smar, Alger.

https://bit.ly/3qzbHjC

La 7ème édition de l'événement international Bsides Algiers aura lieu dans les prochains jours.

L'objectif de cet évènement et de regrouper les passionnés de la cybersécurité et tous ceux qui veulent apprendre et échanger ou même créer une communauté.

Durant cet évènement, il y aura des conférences professionnelles, des ateliers pratiques et des espaces ouverts pour débattre et échanger ainsi qu'une compétition CTF.

Référence	ANPT-2021-BV-12
Titre	Bulletin de veille N°12
Date de version	30 Décembre 2021
Contact	ssi@anpt.dz