BULLETIN DE VEILLE N°01

ANPT-2023-BV-01

"The five most efficient cyber defenders are : Anticipation, Education, Detection, Reaction and Resilience. Do remember: "Cybersecurity is much more than an IT topic."
-- Stephane Nappo --

Janvier 2023

Alertes de sécurité

Lexmark

Une vulnérabilité critique affecte plus de 120 imprimantes Lexmark

27 Janvier 2023

Le fabricant d'imprimantes et de produits d'imagerie Lexmark signale une vulnérabilité d'exécution de code à distance (RCE) affectant plus de 120 modèles d'imprimantes, pour laquelle un code PoC a été publié.

Le problème, suivi sous le nom de CVE-2023-23560 (score CVSS de 9.0), est décrit comme une faille de falsification de requête côté serveur (SSRF) dans la fonction Services Web des appareils Lexmark les plus récents, qui pourrait être exploitée pour exécuter du code arbitraire.

Le fabricant énumère environ 125 modèles d'appareils touchés par ce défaut de sécurité, notamment les imprimantes des séries B, C, CS, CX, M, MB, MC, MS, MX, XC et XM.

Lexmark indique que l'exploitation de la faille peut être bloquée en désactivant la fonction Services Web sur les imprimantes vulnérables (port TCP 65002).

La société a annoncé des mises à jour de micrologiciels qui résolvent la vulnérabilité sur tous les appareils, il est donc conseillé aux utilisateurs d'appliquer les correctifs disponibles dès que possible.

Source : *https://bit.ly/40f4F4i*

Microsoft

Microsoft demande aux clients de mettre à jour leurs serveurs Exchange

27 Janvier 2023

Microsoft a publié un billet de blog pour rappeler à ses clients la vague continue d'attaques visant les serveurs Exchange et pour les inciter à installer les dernières mises à jour disponibles dès que possible.

Le géant technologique a noté que les attaquants ne cherchent pas seulement les informations sensibles que les Mailboxes des utilisateurs peuvent contenir. Ils cherchent également à accéder à la copie du carnet d'adresses de l'entreprise stockée sur le serveur Exchange, qu'ils peuvent ensuite utiliser dans des attaques d'ingénierie sociale.

En plus de cela, Microsoft note que Exchange a des crochets profonds et des permissions dans Active Directory, et dans un environnement hybride, un accès à l'environnement cloud connecté.

Pour mettre à jour un serveur Exchange, les clients doivent commencer par lire l'annonce concernant cette mise à jour, suivre les conseils disponibles pour les mises à jour cumulative CU et les mises à jour de sécurité SU, inventorier tous les serveurs à l'aide de Health Checker et utiliser l'assistant de mise à jour d'Exchange, qui offre un guide étape par étape pour les mises à jour d'Exchange.

Windows Server et les autres logiciels fonctionnant sur le serveur Exchange doivent également être mis à jour, ainsi que les serveurs de dépendance utilisés par Exchange, comme Active Directory et DNS.

Source : *https://bit.ly/3jcC8vG*

BIND

BIND corrige des failles DoS de haute gravité et exploitables à distance

27 Janvier 2023

L'Internet Systems Consortium (ISC) a annoncé des correctifs pour de multiples failles de déni de service (DoS) de haute gravité dans BIND le logiciel pour serveurs DNS.
Les problèmes abordés pourraient être exploités à distance pour provoquer le plantage de named - le démon BIND qui agit à la fois comme authoritative name server et comme recursive resolver - ou pourraient conduire à l'épuisement de la mémoire disponible.
Le premier défaut de sécurité, connu sous le nom de CVE-2022-3094, peut être exploité par l'envoi d'un flot de mises à jour DNS dynamiques, ce qui obligerait named à allouer de

grandes quantités de mémoire, entraînant un plantage dû à un manque de mémoire libre. Pour BIND 9.11 et les branches antérieures, la faille peut être exploitée pour épuiser les ressources internes, ce qui entraîne des problèmes de performance, mais pas de crash.
Répertorié sous le nom de CVE-2022-3736, le second problème conduit à un crash. Un attaquant distant peut déclencher le bogue en envoyant des requêtes modifiées au résolveur.
La troisième vulnérabilité, CVE-2022-3924, affecte l'implémentation de l'option stale-answer-client-timeout, lorsque le résolveur reçoit trop de requêtes nécessitant une récursion, ce qui provoque le plantage de named.
Ces trois vulnérabilités ont été résolues avec la publication des versions 9.16.37, 9.18.11 et 9.19.9 de BIND.
ISC met également en garde contre CVE-2022-3488, un bogue ayant un impact sur toutes les versions de l'édition préliminaire de BIND prises en charge. Le problème peut être déclenché en envoyant deux réponses en succession rapide à partir du même serveur de noms, provoquant le plantage de named.
La version 9.16.37-S1 de l'édition préliminaire de BIND résout les quatre défauts de sécurité. Tous les utilisateurs doivent mettre à jour leurs installations BIND dès que possible.

Source : *https://bit.ly/407ylRb*

Cisco

Cisco corrige une vulnérabilité de haute gravité d'injection SQL dans Unified CM

19 Janvier 2023

Cisco a annoncé des correctifs pour une vulnérabilité d'injection SQL de haute gravité dans Unified Communications Manager (CM) et Unified Communications Manager Session Management Edition (CM SME).

Conçus comme des plateformes de gestion des appels et des sessions d'entreprise, Cisco Unified CM et Unified CM SME assurent l'interopérabilité d'applications telles que Webex, Jabber, et plus encore, tout en maintenant la disponibilité et la sécurité.

Répertoriée sous le nom de CVE-2023-20010 (score CVSS de 8.1), la vulnérabilité est due à une validation incorrecte des entrées utilisateur dans l'interface de gestion Web des plates-formes. Le bogue permet à un attaquant distant et authentifié de lancer une attaque par injection SQL sur un système vulnérable.

Une exploitation réussie pourrait permettre à l'attaquant de lire ou de modifier toutes les données de la base de données sous-jacente ou d'élever ses privilèges.

Le défaut de sécurité affecte Cisco Unified CM et Unified CM SME versions 11.5(1), 12.5(1), et 14, et a été corrigé dans la version 12.5(1)SU7 des applications. Un correctif sera également inclus dans la version 14SU3, qui est prévue pour mars 2023.

Le géant technologique a également informé ses clients d'une vulnérabilité de gravité moyenne de contournement du filtrage des URL dans le logiciel AsyncOS pour Email Security Appliance (ESA). Un attaquant distant et non authentifié pourrait exploiter ce bogue en utilisant des URL modifiés.

Cisco a également annoncé des correctifs pour trois bogues de gravité moyenne dans Expressway Series et TelePresence Video Communication Server (VCS).

Ayant un impact sur l'API et les interfaces de gestion Web de ces produits, les failles pourraient être exploitées par un attaquant distant et authentifié pour écrire des fichiers ou accéder à des données sensibles sur un périphérique vulnérable. Toutes les versions des séries Expressway et TelePresence VCS antérieures à 14.0.7 sont concernées.

Cisco indique qu'à sa connaissance, aucune de ces vulnérabilités n'a été exploitée dans la nature. De plus amples informations sur ces failles sont disponibles sur la page de sécurité des produits de Cisco.

Source : *https://bit.ly/3HJrO85*

Git

Git corrige deux failles de sécurité critiques d'exécution de code à distance

17 Janvier 2023

Le logiciel de gestion de versions décentralisé Git a corrigé deux vulnérabilités de sécurité de gravité critique qui pouvaient permettre aux attaquants d'exécuter du code arbitraire après avoir exploité avec succès des faiblesses de débordement de tampon basées sur le tas.

Les deux premières vulnérabilités (CVE-2022-41903 dans le mécanisme de formatage de commit et CVE-2022-23521 dans l'analyseur .gitattributes) ont été corrigées dans de nouvelles versions remontant à la v2.30.7.

Le troisième, suivi sous le nom de CVE-2022-41953, causée par une faiblesse du chemin de recherche non fiable, permet aux acteurs de la menace non authentifiés d'exécuter des attaques peu complexes de code non fiable, elle est toujours en attente d'un correctif, mais les utilisateurs peuvent contourner le problème en n'utilisant pas le logiciel Git GUI pour cloner des dépôts ou en évitant de cloner à partir de sources non fiables.

Les experts en sécurité de X41 (Eric Sesterhenn et Markus Vervier) et de GitLab (Joern Schneeweisz) ont découvert ces vulnérabilités dans le cadre d'un audit de sécurité du code source de Git parrainé par l'OSTIF.

Le problème le plus grave découvert permet à un attaquant de déclencher une corruption de mémoire basée sur le tas lors d'opérations de clonage ou de tirage, ce qui peut entraîner l'exécution de code. Un autre problème critique permet l'exécution de code pendant une opération d'archivage, qui est couramment effectuée par les forges Git.

En outre, un très grand nombre de problèmes liés aux entiers a été identifié, ce qui peut conduire à des situations de déni de service, des lectures hors limites ou simplement des cas de coin mal gérés sur des entrées importantes.

Dans tous les cas, le moyen le plus efficace de se défendre contre les attaques tentant d'exploiter ces vulnérabilités est de mettre à jour les systèmes vers la dernière version Git (v2.39.1).

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

Actualité

Nouvelle vague d'attaques par injection de base de données visant les sites WordPress

Une importante campagne utilise des sites WordPress piratés pour attirer les consommateurs vers des arnaques d'hameçonnage, de téléchargements illégaux, de sites de rencontres pour adultes et d'assistance technique. Grâce à plusieurs redirections et à des téléchargements légaux, les attaquants se sont assurés que leurs charges utiles malveillantes soient difficiles à détecter.

Selon les experts de Sucuri, le nombre d'infections de sites Web WordPress liées au domaine malveillant violetlovelines[.]com a augmenté. Et les statistiques de PublicWWW ont révélé que depuis le début de la campagne, le 26 décembre 2022, plus de 5 600 sites Web ont été touchés.

La campagne a récemment changé et s'est régulièrement éloignée des pages frauduleuses qui utilisaient de fausses notifications push CAPTCHA vers des réseaux publicitaires black hat. Ces réseaux trompent les utilisateurs pour qu'ils téléchargent des logiciels malveillants en les redirigeant vers des sites Web dignes de confiance, suspects ou dangereux.

La campagne passe par différentes phases pour construire des chaînes de redirection, des réseaux publicitaires, des injections de script et un système de direction du trafic (TDS).

Les injections de balises de script simples et les injections de JavaScript avec obfuscation sont les deux types d'injections les plus fréquemment utilisés par les acteurs de la menace.

La redirection amène les utilisateurs vers un script sur un autre sous-domaine géré par l'attaquant, qui les dirige ensuite vers l'un des nombreux sites du réseau publicitaire malveillant ou vers le TDS.

Pour les sites WordPress infectés gérés par des entreprises des secteurs des jeux, de l'actualité, du commerce électronique, de la pharmacie et des crypto-monnaies, le TDS agit comme un réseau publicitaire.

Ces publicités intrusives encouragent les utilisateurs à télécharger des logiciels sûrs, comme Clean Blocker (une extension de navigateur prétendant être un bloqueur de publicité), et elles incitent aussi les utilisateurs de sites Web à mettre à jour leur navigateur Firefox, Google Chrome ou Microsoft Edge.

Le but ultime de ces publicités est de diffuser des logiciels malveillants qui épuisent les portefeuilles de bitcoins, volent les informations d'identification enregistrées et détournent les sessions de navigation ouvertes sur les ordinateurs des victimes.

Les acteurs de la menace ont propagé Raccoon Stealer en un seul incident et ont pris le contrôle de portefeuilles de crypto-monnaies, de Twitter, de Substack, de Gmail et de Discord.

En outre, les acteurs de la menace utilisent activement des publicités payantes pour inciter les gens à installer ces logiciels malveillants, en utilisant fréquemment des comptes Gmail et des informations de carte de crédit compromis.

Il est conseillé aux utilisateurs de corriger les vulnérabilités connues dès que possible, car cette campagne exploite une grande variété de faiblesses dans les thèmes et plugins WordPress.

Source : *http://bit.ly/3XS3tlV*

Zendesk a été piraté suite à une attaque de phishing

Le fournisseur de solutions d'assistance client Zendesk a connu une violation de données suite à un phishing des identifiants de comptes d'employés.

La société de négociation de crypto-monnaies et de gestion de portefeuille Coinigy a révélé que Zendesk l'avait prévenue d'une violation de la cybersécurité, et qu'elle a découvert le 25 octobre 2022 que plusieurs employés avaient été victimes d'une "attaque sophistiquée de phishing par SMS".

Selon l'email envoyé à Coinigy, les attaquants ont pu accéder aux données non structurées d'une plateforme de journalisation grâce à plusieurs employés qui sont tombés dans le piège et leur ont donné leurs informations de connexion.

Zendesk a déclaré que, dans le cadre de son examen en cours, a découvert des données de service appartenant au compte de l'entreprise peuvent avoir été dans les données de la plate-forme de journalisation. Mais rien n'indiquait que l'instance Zendesk de Coinigy avait été consultée.

Sur la base des informations disponibles, il est toutefois possible que l'attaque contre Zendesk soit liée à la campagne 0ktapus, dans laquelle un acteur de la menace avec une motivation financière apparente a ciblé plus de 130 organisations entre mars et août 2022, y compris des entreprises bien connues comme Twilio et Cloudflare.

Les sociétés de crypto-monnaies figuraient parmi les victimes des attaquants de 0ktapus, qui ont utilisé des messages de phishing basés sur des SMS pour voler les informations de connexion des employés.

Ce n'est pas la première violation de données que Zendesk reconnaît. L'entreprise a révélé en 2019 qu'elle avait eu connaissance d'une violation de sécurité qui a affecté environ 10 000 comptes.

Source : *http://bit.ly/3JsF41R*

GoTo : subit une violation de données

GoTo (anciennement LogMeIn), la société propriétaire de LastPass (un gestionnaire de mot de passe), a révélé que lors d'un incident survenu en novembre 2022, des acteurs de la menace inconnus ont pu acquérir des copies cryptées des données de certains clients ainsi qu'une clé de chiffrement pour certaines de ces sauvegardes.

La violation, qui visait un service tiers de stockage en cloud, a affecté les produits Central, Pro, join.me, Hamachi et RemotelyAnywhere, a déclaré la société.

Selon Paddy Srinivasan de GoTo, "les informations affectées, qui varient selon les produits, peuvent inclure des noms d'utilisateur de compte, des mots de passe salés et hachés, certains paramètres d'authentification multifactorielle (MFA), ainsi que certains paramètres de produits et informations de licence."

Bien qu'il n'y ait aucune preuve que les bases de données cryptées liées aux deux services aient été compromises, les paramètres MFA d'une partie de ses clients Rescue et GoToMyPC ont également été affectés.

L'entreprise n'a pas précisé combien d'utilisateurs ont été touchés, mais elle a dit qu'elle contactait les victimes individuellement pour leur donner plus de détails et leur suggérer quelques "mesures à prendre" pour sécuriser leurs comptes.

GoTo a également été jusqu'à changer les mots de passe des utilisateurs touchés et à leur demander de reconfirmer leurs paramètres MFA. Elle a ajouté qu'elle transférait leurs comptes vers une technologie de gestion d'identité plus avancée, qui promet d'offrir une sécurité plus forte.

L'éditeur de logiciels d'entreprise a précisé qu'il ne conservait pas toutes les informations relatives aux cartes de crédit et ne recueillait pas de données personnelles telles que les dates de naissance, les adresses et les numéros de sécurité sociale.

En décembre 2022, LastPass a également révélé que l'attaquant avait utilisé les données obtenues lors d'un précédent piratage en août pour accéder à un cache important de données de clients, y compris une sauvegarde de leurs coffres-forts de mots de passe cryptés.

Il a été déclaré que les informations obtenues ont été "utilisées pour cibler un autre employé, en recueillant des informations d'identification et des clés qui ont été utilisées pour accéder et décrypter divers volumes de stockage dans le service de stockage en cloud."

Source : *http://bit.ly/3Yd2BrJ*

Les chercheurs avertissent que ChatGPT pourrait créer des malwares polymorphe

Selon les experts en sécurité, le robot d'intelligence artificielle ChatGPT récemment publié par OpenAI pourrait être exploité pour introduire une nouvelle vague dangereuse de logiciels malveillants polymorphes.

Les experts de CyberArk estiment que l'une des nombreuses astuces étonnantes que ChatGPT a réussi à mettre en place consiste à créer des logiciels malveillants incroyablement sophistiqués qui ne contiennent en fait aucun code dangereux, ce qui les rend difficiles à détecter et à atténuer.

« Le concept de création de logiciels malveillants polymorphes à l'aide de ChatGPT peut sembler décourageant, mais en réalité, sa mise en œuvre est relativement simple. En utilisant la capacité de ChatGPT à générer diverses techniques de persistance, des modules anti-VM et d'autres charges utiles malveillantes, les possibilités de développement de logiciels malveillants sont vastes. », a déclaré les experts de CyberArk.

L'utilisation de l'API de ChatGPT dans les logiciels malveillants pourrait poser de sérieuses difficultés aux professionnels de la sécurité. Il est essentiel de garder à l'esprit qu'il s'agit d'un danger très réel, et non d'un simple scénario hypothétique.

Source : *http://bit.ly/40jW7cO*

Bon à savoir

La formation et la gestion des terminaux réduisent les risques de cybersécurité du télétravail

Selon une étude faite par Hornetsecurity, 33 % des entreprises ne forment pas leurs travailleurs à distance à la cybersécurité, alors que 74% de ses employés ont accès à des informations sensibles, ce qui augmente le danger pour les entreprises dans le nouveau lieu de travail hybride.

"En raison de la popularité croissante du travail hybride et des risques qu'il comporte, les entreprises doivent accorder une priorité absolue à la formation et à l'éducation afin de sécuriser le travail à distance. Lorsque les employés travaillent à distance, les contrôles et les mesures de sécurité traditionnels sont moins efficaces, et la responsabilité incombe davantage à l'individu. " a déclaré Daniel Hofmann, PDG de Hornetsecurity, "les entreprises doivent reconnaître les dangers distincts liés au travail à distance et activer des solutions de gestion de la sécurité pertinentes, ainsi que permettre aux employés de faire face à un certain niveau de risque."

L'accès des employés à des données sensibles et l'insuffisance de la formation à la gestion de la cybersécurité et à l'atténuation du danger d'une cyberattaque ou d'une violation sont les deux principaux facteurs de risque.

Hofmann a commenté : "Le renforcement des mesures de cybersécurité du travail à distance est particulièrement important dans le climat actuel, car les cybercriminels deviennent plus intelligents et utilisent le travail à distance à leur avantage. Nous avons constaté une augmentation des attaques par smartphone, les pirates ayant compris que les données personnelles et professionnelles sont susceptibles d'être consultées, car les gens peuvent, et le font souvent, effectuer des travaux sur des appareils personnels."

Les spécialistes savent que le travail à distance pose des problèmes particuliers, mais les gens subissent les conséquences de mesures de protection inadéquates et d'une gestion à distance insuffisante.

Selon l'enquête, seulement 14 % des personnes interrogées ont déclaré que leur organisation avait subi un incident de cybersécurité lié au travail à distance.

L'étude a également mis en évidence un manque de compréhension, de confiance et de connaissances en matière de cybersécurité de la part des employés qui travaillent à distance. 43 % des professionnels de l'informatique estiment que leur confiance dans leurs mesures de sécurité à distance est "modérée" ou pire. De plus, cette étude révèle que le "partage incontrôlé de fichiers" est une source courante d'incidents de cybersécurité (16 %).

Les organisations peuvent réduire les risques liés à la cybersécurité en améliorant la formation et l'éducation. Une instruction de base pourrait grandement améliorer la situation.

Il est important de mettre en place des systèmes solides pour protéger les employés. L'étude a montré que les principales sources d'incidents de cybersécurité étaient les points d'extrémité compromis (28 %) et les informations d'identification compromises (28 %). En outre, 15 % ont déclaré que les employés utilisent leurs propres appareils avec une certaine configuration des terminaux pour le travail à distance.

Les systèmes de gestion des terminaux et les formations de sensibilisation à la sécurité sont indispensables aux entreprises pour assurer la cybersécurité à distance.

Source : *http://bit.ly/3RhqYCD*

Evènements

Evènement du mois

Formation à la cybersécurité : Sécuriser votre réseau domestique

31 Janvier 2023

Online

https://bit.ly/3DrC1TU

Un réseau domestique sécurisé constitue un aspect essentiel de la sécurité Internet. Les cybercriminels peuvent exploiter les réseaux vulnérables pour mettre en œuvre un éventail de cybercrimes, comme l'installation d'un programme malveillant, le vol de données, l'usurpation d'identité et la création de botnets.

L'objectif de cet événement est de savoir comment le réseau domestique est configuré et de prendre des mesures pour le rendre aussi sûr et sécurisé que possible.

Evènement à venir

Les fondamentaux de la cybersécurité pour les professionnels de l'informatique

06 Fevrier 2023

Online

https://bit.ly/3Ybx7lX

Alors que les organisations adoptent la transformation numérique, les cybercriminels font de même. Les cyber-activités malveillantes ont évolué en sophistication, et la furtivité et le travail d'équipe sont nécessaires pour contourner les cybermenaces et les attaques.

Ce cours en ligne couvre un large éventail de domaines clés de la cybersécurité qui sont essentiels pour les professionnels de l'informatique, il a été conçu pour aider les apprenants à développer une compréhension approfondie de la cybersécurité, des vecteurs d'attaque, des contrôles, de la protection des données, de la confidentialité des données et des systèmes de gestion de la sécurité de l'information.

Référence	ANPT-2023-BV-01
Titre	Bulletin de veille N°01
Date de version	31 Janvier 2023
Contact	ssi@anpt.dz