BULLETIN DE VEILLE N°12

ANPT-2022-BV-12

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

Décembre 2022

Alertes de sécurité

WordPress

Des pirates ciblent Gift Cardde plugin de WordPress pour télécharger des Backdoors

28 Décembre 2022

Des cyberpirates exploitent activement une vulnérabilité critique dans le plugin WordPress YITH WooCommerce Gift Cards Premium pour télécharger des backdoors sur les boutiques en ligne. Ce plugin permet aux boutiques en ligne de vendre des cartes cadeaux, utilisées par des dizaines de milliers de sites web.

Les attaquants ont exploité la faille en envoyant des requêtes POST à /wp-admin/admin-post.php, ce qui leur a permis de télécharger un exécutable PHP malveillant sur le site.

La faille est sous le nom de CVE-2022-4539, et se trouve dans la fonction "import_actions_from_settings_panel" du plugin qui s'exécute sur la fonction "admin_init".

L'exploitation de ce bogue permet à un attaquant de télécharger des fichiers, y compris des shells web, sur des sites vulnérables.

Plus de 50 000 sites web utilisent encore les versions vulnérables du plugin, ce qui permet aux acteurs de la menace d'explorer la faille et de placer une backdoor pour lancer des attaques par exécution de code à distance et prendre le contrôle de sites.

Il est conseillé aux utilisateurs ayant des versions de site défectueuses de passer à la version 3.20.2 du plugin WordPress YITH WooCommerce Gift Cards pour rester en sécurité.

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

ZyXEL

Une porte Backdoor trouvées dans le routeur ZyXEL

27 Décembre 2022

Un chercheur a découvert une backdoor cachée dans les routeurs d'intérieur ZyXEL LTE. La backdoor codée en dur, connue sous le nom de CVE-2022-40602, permet un accès à distance à tout attaquant.

Le chercheur (ReSolver) a découvert le mot de passe caché dans le firmware des routeurs ZyXEL LTE3301-M209. Le firmware de cet appareil, qui comprend trois sections principales : la section LZMA, le root-fs et le contenu www, contient un fichier contenant les informations d'identification.

Le fichier, stocké dans la section www content de la section firmware, contient les octets magiques Zlib.

Ces octets magiques Zlib peuvent être lus à l'aide des utilitaires OpenSSL ou zlib-flate sous Unix. Alternativement, sous Windows OS, un utilisateur peut convertir le fichier zlib en un fichier gzip puis le lire en utilisant 7zip.

Lorsque le chercheur a décompressé le fichier, il a exposé le mot de passe de connexion telnet. De plus, il y avait des identifiants WebUI (identifiants WebUI/telnet) qui pouvaient permettre à l'attaquant de posséder l'appareil.

Le même expert a trouvé une porte dérobée Telnet dans le DWR-921 de D-Link également. L'entreprise a publié un bulletin de sécurité et un correctif de firmware.

Les utilisateurs de routeurs vulnérables sont invités à appliquer le correctif immédiatement. Par ailleurs, la coordination entre le chercheur et ZyXEL met en évidence le fait qu'une communication et une collaboration claires entre ces deux sujets complémentaires peuvent réduire de manière significative les risques d'exploitation de tels bugs dans la nature.

Source : *https://bit.ly/3hSaa83*

Ghost CMS

Contournement d'authentification et vulnérabilités d'énumération dans Ghost CMS

21 Décembre 2022

Cisco Talos a récemment découvert deux vulnérabilités dans le Ghost CMS, une vulnérabilité de contournement d'authentification et une vulnérabilité d'énumération.

Ghost est un système de gestion de contenu avec des outils permettant de construire un site web, de publier du contenu et d'envoyer des newsletters. Ghost propose des abonnements payants aux membres et prend en charge un certain nombre d'intégrations avec des services externes.

La vulnérabilité peut conduire à une augmentation des privilèges. TALOS-2022-1624 (CVE-2022-41654) permet aux utilisateurs externes de mettre à jour leurs préférences de newsletter de manière trop libérale, ce qui pourrait permettre à un utilisateur un accès complet pour créer et modifier les newsletters, y compris la valeur par défaut envoyée à tous les membres.

TALOS-2022-1625 (CVE-2022-41697) est une vulnérabilité d'énumération dans la fonctionnalité de connexion de Ghost qui peut conduire à une divulgation d'informations sensibles.

Un attaquant peut envoyer des requêtes HTTP pour déclencher ces vulnérabilités.

Les utilisateurs sont incités à mettre à jour ce produit affecté (Ghost Foundation Ghost 5.9.4) dès que possible.

Source : https://bit.ly/3VvuuK7

Citrix

Des milliers de serveurs Citrix vulnérables aux failles critiques corrigées

28 Décembre 2022

Des milliers de déploiements de Citrix ADC et Gateway restent vulnérables à deux problèmes de sécurité de gravité critique.

La première faille est CVE-2022-27510, il s'agit d'un contournement d'authentification qui affecte les deux produits Citrix. Un attaquant pourrait l'exploiter pour obtenir un accès non autorisé à l'appareil, effectuer une prise de contrôle du bureau à distance ou contourner la protection par force brute de la connexion.

Le deuxième bogue est répertorié sous le nom de CVE-2022-27518 touche la version la 12.1-65.21, il permet à des attaquants non authentifiés d'exécuter des commandes à distance sur des appareils vulnérables et d'en prendre le contrôle.

Les statistiques indiquent qu'au 28 décembre 2022, la majorité des serveurs Citrix qui se trouvent sur la version 13.0-88.14, ne sont pas affectée par les deux problèmes de sécurité.

L'équipe Fox IT de NCC Group espère que son blog contribuera à sensibiliser les administrateurs Citrix qui n'ont pas encore appliqué les mises à jour de sécurité pour les récentes failles critiques, car malgré que la plupart des terminaux Citrix destinés au public ont été mis à jour vers une version fiable, mais des milliers d'entre eux restent vulnérables aux attaques, les statistiques soulignant qu'il reste encore beaucoup à faire pour combler toutes les failles de sécurité.

Source : https://bit.ly/3i0dSME

Rockwell Automation

Plusieurs vulnérabilités DoS et d'exécution de code découvertes dans les contrôleurs de Rockwell Automation

29 Décembre 2022

L'agence américaine de cybersécurité et de sécurité des infrastructures (CISA) a publié trois avis décrivant un total de quatre vulnérabilités de haute gravité. Rockwell Automation (un fournisseur d'envergure mondial de solutions d'automatisation industrielle, de puissance, de contrôle et d'information) a publié des avis individuels pour chaque faille de sécurité.

Des chercheurs du Veermata Jijabai Technological Institute (VJTI) et du Georgia Institute of Technology qui ont signalé les vulnérabilités des automates MicroLogix à Rockwell.

La première faille est la CVE-2022-3156, qui a un impact sur le logiciel d'émulation du contrôleur Studio 5000 Logix Emulate. La vulnérabilité est due à une mauvaise configuration qui fait que les utilisateurs se voient accorder des autorisations élevées sur certains services du produit. Un attaquant pourrait exploiter cette faiblesse pour exécuter du code à distance.

La deuxième vulnérabilité est CVE-2022-3157, qui affecte les contrôleurs CompactLogix, GuardLogix (y compris Compact) et ControlLogix. Un attaquant peut exploiter la faille pour lancer une attaque par déni de service (DoS) contre un périphérique en envoyant des requêtes CIP spécialement conçues qui provoquent une "major non-recoverable fault".

Les autres failles ont un impact sur les automates programmables (PLC) MicroLogix 1100 et 1400. L'une des failles de sécurité, CVE-2022-46670, est un problème de cross-site scripting (XSS) stocké dans le serveur web embarqué qui peut être exploité pour l'exécution de code à distance sans authentification. La deuxième est CVE-2022-3166, c'est un problème de clickjacking qui peut être exploité par un attaquant ayant un accès réseau à l'appareil affecté pour provoquer une condition DoS pour l'application du serveur web.

Les deux premières vulnérabilités ont été corrigées par des mises à jour. Pour les deux dernières, le fournisseur a mis à disposition des mesures d'atténuation qui devraient empêcher les attaques.

Source : https://bit.ly/3jD0O0j

Microsoft

Le Patch Tuesday de décembre 2022 de Microsoft corrige 2 zero-days, 49 failles

13 Décembre 2022

Le Patch Tuesday de Microsoft corrige deux vulnérabilités de type "zero day", dont un bogue activement exploité, et un total de 49 failles.

La première vulnérabilité zero day est CVE-2022-44698, un contournement de la fonctionnalité de sécurité de Windows SmartScreen découverte par Will Dormann.

La deuxième est sous le nom de CVE-2022-44710, une vulnérabilité d'élévation de privilège du noyau graphique de DirectX, découverte par Luka Pribanić.

Six des 49 vulnérabilités corrigées sont classées comme "critiques" car elles permettent l'exécution de code à distance, l'un des types de vulnérabilités les plus graves.

- 19 vulnérabilités d'élévation de privilèges ;
- 23 vulnérabilités d'exécution de code à distance ;
- 2 vulnérabilités de contournement des fonctions de sécurité ;
- 3 vulnérabilités liées à la divulgation d'informations ;
- 3 vulnérabilités de déni de service ;
- 1 vulnérabilité d'usurpation d'identité.

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

Actualité

Twitter : un attaquant affirme avoir récupéré les données de 400 millions d'utilisateurs

Sur un forum dédié aux violations criminelles de données, un post demande à Elon Musk d'acheter un ensemble de données pour une somme indéfinie, après avoir affirmé avoir obtenu les adresses électroniques et les numéros de téléphone de 400 millions d'utilisateurs de Twitter.

Le message comprend les adresses électroniques privées présumées de trente-deux personnes connues, dont Alexandria Ocasio-Cortez, députée démocrate de New York, Vitalik Buterin, fondateur de la crypto-monnaie Ethereum, et Brian Krebs, journaliste spécialisé dans la cybersécurité. Le message aurait été découvert par la société israélienne de cyberespionnage Hudson Rock.

Le message contient également un lien vers une feuille de calcul contenant 1 000 enregistrements, dont certains appartiennent à des entités publiques et dont les adresses électroniques fournies semblent authentiques.

L'auteur du message, qui se fait appeler "Ryushi" et a un avatar masculin, affirme que les enregistrements ont été mis à disposition pour le raclage "par le biais d'une vulnérabilité", mais il n'a pas réagi à une demande de clarification sur son canal Telegram.

Si la fuite de données est confirmée, il s'agira d'un nouveau revers pour Twitter et son PDG en difficulté, qui a déclaré qu'il se retirerait de la gestion de la plateforme tout en restant propriétaire.

Twitter a accepté un décret de consentement avec la Commission fédérale du commerce des États-Unis qui l'oblige à maintenir un programme de protection de la vie privée et de sécurité de l'information pendant les 20 prochaines années. L'accord a mis fin à une enquête fédérale sur l'utilisation par Twitter des numéros de téléphone et des adresses électroniques acquis pour l'authentification multifactorielle à des fins publicitaires. Twitter a également payé une amende civile de 150 millions de dollars. Selon Bloomberg, l'agence intensifie son enquête pour déterminer si Twitter respecte l'ordonnance, en particulier à la lumière du départ d'employés de haut niveau dans les domaines du droit, de la confidentialité et de la conformité.

Les coordonnées de 5,4 millions d'utilisateurs de Twitter ont été publiées sur un site fréquenté par Ryushi dans le cadre d'un incident signalé à la Commission irlandaise de protection des données.

Selon le régulateur irlandais de la protection des données, Twitter semble avoir enfreint le règlement général sur la protection des données, une loi européenne sur la protection de la vie privée fréquemment sanctionnée par de fortes amendes. Invoquant le GDPR, l'agence irlandaise a infligé une amende de 265 millions d'euros à Facebook en novembre après qu'une collecte de données comprenant les informations personnelles de plus de 500 millions d'utilisateurs du réseau social ait fait surface en ligne l'année précédente.

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

Un ransomware utilise un nouvel exploit pour contourner les mesures d'atténuation de ProxyNotShell

Une nouvelle chaîne d'exploitation qui va au-delà des mesures d'atténuation de ProxyNotShell de Microsoft a été utilisée dans les récentes attaques de ransomware de Play qui ciblent les serveurs Exchange.

ProxyNotShell est une paire de failles de sécurité dans Exchange Server qui sont comparables à la précédente vulnérabilité ProxyShell. Ces failles sont CVE-2022-41040, un bug de falsification de requête côté serveur (SSRF) avec un score CVSS de 8,8, et CVE-2022-41082, un bug d'exécution de code à distance (RCE) avec un score CVSS de 8,0.

Les deux failles ont été identifiées pour la première fois en septembre, mais les attaques en tiraient déjà parti. Elles ont été corrigées dans le Patch Tuesday de novembre 2022 de Microsoft avec plusieurs problèmes.

Afin d'accéder au point de terminaison Autodiscover et au backend Exchange pour n'importe quelle URL, la chaîne d'attaque ProxyNotShell cible CVE-2022-41040. Ensuite, CVE-2022-41082 est exploité pour permettre l'exécution de code arbitraire. En réponse, Microsoft a mis en œuvre un certain nombre de mesures d'atténuation de la réécriture d'URL pour le point de terminaison Autodiscover.

Cependant, les attaques de ransomware Play obtiennent un accès au début grâce à une nouvelle chaîne d'exploitation que CrowdStrike a baptisée OWASSRF. Cette chaîne d'exploitation se compose d'un SSRF identique à l'approche Autodiscover et de la vulnérabilité utilisée dans la deuxième phase de ProxyNotShell.

Au lieu d'utiliser Autodiscover, OWASSRF permet aux attaquants d'accéder au service de remoting PowerShell via l'application Web Outlook (OWA). Selon l'entreprise de cybersécurité, l'attaque utilise très probablement CVE-2022-41080, un bug d'escalade de privilèges de haute gravité affectant Exchange Server 2016 et 2019.

Le 8 novembre, CVE-2022-41080 a été patché en même temps que les vulnérabilités ProxyNotShell et une autre faiblesse d'escalade de privilèges connue sous le nom de CVE-2022-41123, également connue sous le nom de bug de détournement de DLL.

"CVE-2022-41080 n'a pas été décrit publiquement, mais il a été signalé comme ayant une plus grande probabilité d'être exploité en raison de son score CVSS similaire de 8,8 à celui de CVE-2022-41040, qui a été utilisé dans la chaîne d'exploitation ProxyNotShell. Selon ces résultats, CrowdStrike détermine qu'il est très probable que l'approche OWA utilisée soit effectivement liée à CVE-2022-41080.

Il est conseillé aux organisations de déployer des outils de détection et de réponse aux points d'extrémité (EDR) capables d'identifier les tentatives d'exploitation potentielles, d'appliquer dès que possible les correctifs de novembre 2022 de Microsoft, d'atténuer ProxyNotShell et les autres vulnérabilités exploitées, de désactiver PowerShell à distance pour les utilisateurs non administratifs et d'atténuer les autres vulnérabilités exploitées.

Source : *https://bit.ly/3G2Z4EZ*

Des pirates volent des NFT via des sites de phishing

Des attaquants de Corée du Nord volent des actifs numériques d'une valeur de plusieurs milliers de dollars en se faisant passer pour des plateformes de jetons non fongibles et des places de marché de finance décentralisée bien connues sur des sites de phishing.

Selon la société de sécurité blockchain SlowMist, les attaquants ont mis en place environ 500 sites contrefaits, dont un pour un projet lié à la Coupe du monde et les places de marché NFT (Non-Fungible Token) OpenSea, X2Y2 et Rarible. En volant 1 055 NFT à l'aide d'une seule de ces adresses de phishing, ils ont emporté 365 000 dollars. Le montant global des biens volés n'a pas été indiqué.

Selon SlowMist, la campagne de phishing, qui dure depuis au moins sept mois, n'est que "la partie émergée de l'iceberg".

La majorité des casses liés aux cryptomonnaies cette année ont été menés par les groupes de menaces persistantes avancées du pays. Selon un rapport publié en septembre par la startup d'analyse blockchain Chainalysis, des entités liées à la Corée du Nord ont volé 600 millions de dollars au Ronin Network et près d'un milliard de dollars au total via les protocoles DeFi cette année.

Dans certains cas, les attaquants ont produit de faux sites Web liés au NFT avec des monnaies malveillantes destinées à tromper les victimes. Pour tenter de créer un NFT, les utilisateurs connectaient leurs portefeuilles aux faux sites Web, mais au lieu de cela, ils laissaient leurs portefeuilles ouverts aux attaques, donnant à l'attaquant un accès complet aux actifs qu'ils contenaient.

La société affirme que les attaquants ont également gardé la trace des informations des visiteurs et les ont utilisées pour lancer différents scripts d'attaque contre la victime. Les pirates ont ainsi eu accès à des informations sensibles telles que la fiche d'approbation et les sigData de la victime, ainsi que ses journaux d'accès, ses autorisations et son utilisation des portefeuilles de plug-ins. Selon SlowMist, "toutes ces données permettent ensuite au pirate d'accéder au portefeuille de la victime, exposant ainsi tous ses objets de valeur numériques."

Deux adresses IP étaient principalement utilisées par les opposants pour opérer. L'une abritait 320, tandis que la première hébergeait 372 sites de phishing NFT.

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

Bon à savoir

Les principales vulnérabilités de sécurité en 2022

L'environnement des cybermenaces évolue constamment en même temps que la technologie. Pour les équipes de sécurité et de technologie, il est essentiel de rester au courant des failles de sécurité. À l'approche de la nouvelle année, voici les principales vulnérabilités de sécurité que les organisations devraient connaître depuis 2022 :

- Faille MSDT de Follina (CVE-2022-30190) : Ce bogue de type zero-day a été identifié dans les gestionnaires d'URL MS intégrés (ms-msdt :) qui déclenchent le processus Microsoft Support Diagnostic Tool (MSDT) utilisé pour exécuter du code sur le système cible. La solution consiste à supprimer l'entrée de registre responsable de ce problème ;
- Log4Shell/Log4j (CVE-2021-44228) : Ce zero-day donnait aux attaquants la possibilité d'obtenir des privilèges suite à l'exécution du code arbitraire sur un système cible en manipulant les messages du journal. Ce problème a été corrigé dans les versions Log4j 2.3.2 (pour Java 6), 2.12.4 (pour Java 7) ou 2.17.1 (pour Java 8 et ultérieur) ;
- Spring4Shell/Springshell (CVE-2022-22965) : Les applications utilisant la fonction de recherche de données dans le framework spring et exécutant des versions JDK 9+ sont affectées par spring4shell, qui permet au attaqaunt non authentifié l'exécution de code à distance. La version 2.6.6 est le correctif de ce bogue ;
- Faille RCE de BIG-IP (CVE-2022-1388) : Le bogue a été jugée critique, permet l'exécution de code à distance sur les systèmes exécutant l'API iControl REST et les versions affectées de F5 BIG-IP, donnant à l'attaquant un accès complet à ces serveurs. Le fournisseur a mis à disposition un correctif le 4 mai 2022 ;
- Utilisation après libération dans l'animation de Google Chrome (CVE-2022-0609) : Un attaquant distant peut utiliser l'utilisation après libération dans une animation dans les versions vulnérables de Google Chrome (antérieures à 98.0.4758.102) en créant un site web HTML spécialement conçu. Ce type de vulnérabilité provoque une corruption de la mémoire ;
- ProxyNotShell (CVE-2022-41040 et CVE-2022-41082) dans Exchange : Le premier bogue est une faille SSRF (Server-side request forgery), elle permet à un utilisateur authentifié de déclencher à distance le deuxième bogue, qui permet un RCE lorsque PowerShell est accessible à un acteur de la menace ;
- Zimbra RCE (CVE-2022-27925 et CVE-2022-41352) : Les attaquants pourraient profiter de ces failles en envoyant des courriels de phishing avec des pièces jointes ou des liens malveillants qui leur donnent accès à des comptes d'utilisateurs ou à des fichiers système sur un système sensible.

- Vulnérabilité d'Atlassian Confluence (CVE-2022-26134) : De multiples preuves de concept étaient disponibles sur GitHub pour exploiter cette vulnérabilité critique d'exécution de code à distance par injection OGNL non authentifiée qui affectait le serveur et le centre de données Confluence. Ce bogue a été corrigé dans les versions 7.4.17, 7.13.7, 7.14.3, 7.15.2, 7.16.4, 7.17.4 et 7.18.1 de Confluence ;
- Vulnérabilité de ZyXEL (CVE-2022-30525) : Cette faille permettait à un attaquant distant non authentifié de réaliser une exécution de code arbitraire en tant qu'utilisateur nobody sur les pares-feux ZyXEL affectés.

Une approche de la gestion des correctifs basée sur le risque permet de défendre les entreprises contre les failles potentielles que les acteurs malveillants sont impatients d'exploiter rapidement.

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

Evènements

Evènement du mois

Réduire les violations de données Best Practice For Web Application Security

29 Décembre 2022

Online

https://bit.ly/3GqgBIH

La sécurité est devenue plus critique que jamais. Les derniers rapports sur les incidents de violation de données indiquent que les applications web sont devenues la première forme de violation. La question qui se pose souvent est comment savoir si les mesures prises pour protéger les applications web et sécuriser les données sont suffisantes.
Cet événement en ligne traitera de la mise en œuvre d'un processus et d'une méthodologie normalisés pour tester les applications Web d'une manière complète, reproductible et reconnue par l'industrie.

Evènement à venir

Session d'information virtuelle Cybersecurity Certificate Program

17 Janvier 2023

Online

https://bit.ly/3Z7yaVs

La formation de la main-d'œuvre en matière de cybersécurité vise à combler le canal entre les professionnels qui cherchent à faire carrière et les employeurs qui cherchent à embaucher.

Financé par une subvention des National Centers of Academic Excellence en Cybersecurity (situés au sein de la National Security Agency), les cours seront proposés à 100 % en ligne et comprendront des laboratoires d'apprentissage pratiques pour améliorer les compétences en matière de cybersécurité.

Référence	ANPT-2022-BV-12
Titre	Bulletin de veille N°12
Date de version	31 Décembre 2022
Contact	ssi@anpt.dz