BULLETIN DE VEILLE N°09

ANPT-2022-BV-09

"Cyber-Security is much more than a matter of IT."
-- Stephane Nappo --

Septembre 2022

Alertes de sécurité

Microsoft

Microsoft publie un correctif pour une faille permettant les mouvements latéraux et les attaques par ransomware

23 Septembre 2022

Microsoft a publié une mise à jour de sécurité hors bande pour sa solution Endpoint Configuration Manager afin de corriger une vulnérabilité qui pourrait être utile aux acteurs malveillants pour se déplacer dans le réseau d'une organisation ciblée.

La vulnérabilité, connue sous le nom de CVE-2022-37972, a été décrite par Microsoft comme un problème d'usurpation d'identité de gravité moyenne après avoir été signalée par Brandon Colley de Trimarc Security.

Colley a montré comment un attaquant disposant de privilèges d'administrateur sur un terminal pouvait abuser des défauts de conception de l'installation push client pour obtenir les informations d'identification hachées de tous les comptes push Microsoft System Center Configuration Manager configurés.

Certains de ces comptes peuvent avoir des privilèges d'administrateur de domaine ou des privilèges élevés sur plusieurs machines dans l'entreprise, ils peuvent être exploités par des acteurs de la menace pour un mouvement latéral et même dans le cadre d'une attaque de ransomware perturbatrice.

La vulnérabilité de Microsoft Endpoint Configuration Manager corrigée par Microsoft au moyen d'une mise à jour hors bande est liée à l'utilisation de protocole d'authentification NTLM pour le compte push du client.

L'Agence américaine de cybersécurité et de sécurité des infrastructures (CISA) a exhorté les administrateurs à examiner l'avis de Microsoft et à appliquer les mises à jour nécessaires.

Source : *https://bit.ly/3dOv5Xn*

Android

Harly : un autre abonné cheval de Troie sur Google Play

22 Septembre 2022

Il est courant de trouver toutes sortes de logiciels malveillants cachés sous des applications apparemment inoffensives sur la boutique officielle Google Play. Malheureusement, même si la plateforme est surveillée de près, les modérateurs ne peuvent pas toujours attraper ces applications avant qu'elles ne soient publiées. L'une des variantes les plus populaires de ce type de malware est le cheval de Troie, qui permet de s'inscrire à des services payants à l'insu de l'utilisateur. Harly fait partie des familles des Chevaux de Troie.

Depuis 2020, plus de 190 applications infectées par Harly ont été trouvées sur Google Play. Une estimation prudente du nombre de téléchargements de ces apps est de 4,8 millions.

Les escrocs téléchargent des applications ordinaires sur Google Play, y insèrent un code malveillant, puis les transfèrent sur Google Play sous un autre nom. Les applications peuvent présenter les mêmes caractéristiques que celles mentionnées dans la description, de sorte que les utilisateurs ne se doutent pas de la menace.

Harly collecte des informations sur l'appareil de l'utilisateur, et notamment sur le réseau mobile. Le téléphone de l'utilisateur bascule vers un réseau mobile, puis le cheval de Troie demande au serveur C&C de configurer la liste des abonnements auxquels il faut s'inscrire.

Ce cheval de Troie ouvre l'adresse de l'abonnement dans une fenêtre invisible et, en injectant des scripts JS, saisit le numéro de téléphone de l'utilisateur, appuie sur les boutons requis et saisit le code de confirmation d'un SMS. Le résultat est que l'utilisateur obtient un abonnement payant sans s'en rendre compte. Il peut s'abonner non seulement lorsque le processus est protégé par un code de message texte, mais aussi lorsqu'il est protégé par un appel téléphonique : dans ce cas, le cheval de Troie appelle un numéro spécifique et confirme l'abonnement.

Avant d'installer une application, vous devriez d'abord lire les avis des utilisateurs et vérifier son classement sur Google Play. Bien entendu, n'oubliez pas que les avis et les notes peuvent être exagérés. Pour couvrir toutes vos bases afin d'éviter d'être la proie de ce type de malware, Kaspersky vous recommande d'installer sa dernière mise à jour du 06 septembre 2022.

Source : *https://bit.ly/3UKixB2*

Unix

Des vulnérabilités dans une bibliothèque populaire affectent les appareils basés sur Unix

22 Septembre 2022

Cisco Talos a récemment découvert une vulnérabilité de corruption de mémoire dans la bibliothèque uClibC qui pourrait affecter tous les dispositifs basés sur Unix qui utilisent cette bibliothèque. uClibC et uClibC-ng sont des remplacements légers pour la bibliothèque populaire gLibc, qui est l'implémentation de la bibliothèque standard C du projet GNU.

TALOS-2022-1517 (CVE-2022-29503 - CVE-2022-29504) est une vulnérabilité de corruption de mémoire dans uClibC et uClibc-ng qui peut se produire si un utilisateur malveillant crée des threads de manière répétée.

De nombreux dispositifs embarqués utilisent cette bibliothèque, mais Talos a spécifiquement confirmé que le Anker Eufy Homebase 2, version 2.1.8.8h, est affecté par cette vulnérabilité. Anker a confirmé avoir mis en place un correctif pour ce problème. Cependant, uClibC n'a pas publié de correctif officiel, bien que nous divulguions cette vulnérabilité conformément à la politique de divulgation des vulnérabilités de 90 jours de Cisco.

Talos a testé et confirmé que les logiciels suivants sont affectés par ces vulnérabilités : uClibC, version 0.9.33.2 et uClibC-ng, version 1.0.40.

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

Firefox et Thunderbird

Mettez à jour Firefox et Thunderbird maintenant ! Mozilla corrige plusieurs vulnérabilités à haut risque

22 septembre 2022

Mozilla a publié des mises à jour de sécurité pour corriger des vulnérabilités dans Firefox, Firefox ESR et Thunderbird. Un attaquant pourrait exploiter certaines de ces vulnérabilités pour prendre le contrôle d'un système affecté.

Dans Firefox 105, un total de sept vulnérabilités ont été corrigées, dont trois ont reçu la note de risque de sécurité "élevé". Dans Thunderbird, trois vulnérabilités de sécurité ont été corrigées. L'une d'entre elles a reçu la note de risque "élevé".

Des avis de sécurité ont été publiés pour Firefox 105, Firefox ESR 102.3 et Thunderbird 91.13.1. Firefox 105 est le navigateur que la plupart des utilisateurs de Mozilla auront sur leur système. Firefox Extended Support Release (ESR) est une version officielle de Firefox développée pour les grandes organisations qui ont besoin de configurer et de maintenir Firefox à grande échelle. Thunderbird est l'application de messagerie électronique gratuite de Mozilla.

Vulnérabilités de Firefox :

- CVE-2022-40960 : (Elevé) L'utilisation simultanée de l'analyseur d'URL avec des données non-UTF-8 non sécurisée par les threads.
- CVE-2022-40959 : (Elevé) Contournement des restrictions FeaturePolicy sur les pages transitoires.
- CVE-2022-40962 : (Elevé) Des bogues de sécurité mémoire ont été corrigés dans Firefox 105 et Firefox ESR 102.3.
- CVE-2022-40958 : (Modéré) Contournement de la restriction « Secure Context » pour les cookies avec le préfixe __Host et __Secure.
- CVE-2022-40961 : (Modéré) Débordement de tampon de pile causant un crash potentiellement exploitable lors de l'initialisation des graphiques.
- CVE-2022-40956 : (Faible) Contournement de base-uri de Content-Security-Policy (CSP).
- CVE-2022-40957 : (Faible) Cache d'instructions incohérent lors de la construction de WASM sur ARM64. Ce bogue n'affecte que Firefox sur les plateformes ARM64. ARM64 est l'architecture utilisée par les nouveaux Macs construits sur Apple Silicon, livrés à la fin de 2020 et au-delà.

Vulnérabilités de Thunderbird :

- CVE-2022-3033 : (Elevé) Fuite d'informations sensibles lors de la composition d'une réponse à un email HTML avec une balise META refresh. Ce bogue n'affecte pas les utilisateurs qui ont changé le paramètre d'affichage par défaut du corps du message en 'html simple' ou 'plain text'.
- CVE-2022-3032 : (Modéré) Lors de la réception d'un email HTML contenant un élément iframe, qui utilise un attribut srcdoc pour définir le document HTML interne, le réseau sera accessible, et les objets seront chargés et affichés.
- CVE-2022-3034 : (Modéré) Un élément iframe dans un email HTML pourrait déclencher une requête réseau

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

Sophos

Un nouveau bug activement exploité dans le produit Firewall de Sophos

23 Septembre 2022

Sophos signale une vulnérabilité de sécurité critique par injection de code, suivie sous le nom de CVE-2022-3236, affectant son produit Firewall. Cette faille réside dans le portail utilisateur et l'administrateur Web de Sophos Firewall, son exploitation peut conduire à une exécution de code (RCE).

Sophos a observé que cette vulnérabilité était utilisée pour cibler un petit ensemble d'organisations spécifiques, principalement dans la région de l'Asie du Sud.

L'entreprise a résolu le problème avec la version 19.0 MR1 (19.0.1) et les versions antérieures du pare-feu. Elle a également recommandé aux clients de ne pas exposer le portail utilisateur et l'administrateur Web au WAN et de désactiver l'accès WAN au portail utilisateur et à Webadmin. Et utiliser un VPN et/ou Sophos Central (de préférence) pour l'accès et la gestion à distance.

Les clients utilisant des versions plus anciennes de Firewall doivent passer à une version prise en charge.

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

Actualité

Le constructeur du ransomware LockBit a été divulgué en ligne par un "développeur en colère"

Le groupe LockBit ransomware a été victime d'une fuite. En effet, un développeur mécontent aurait divulgué le programme de construction du dernier cryptage du groupe « LockBit version 3.0 ».

Cette nouvelle version promettait de « rendre les ransomwares à nouveau performants », en ajoutant de nouvelles fonctionnalités anti-analyse, un programme de primes pour les bugs de ransomwares et de nouvelles méthodes d'extorsion.

Cependant, il semble que LockBit soit victime d'une violation, deux personnes (ou peut-être la même personne) ayant divulgué le constructeur de LockBit 3.0 sur Twitter.

Selon le chercheur en sécurité 3xp0rt, un utilisateur de Twitter récemment enregistré sous le nom de "Ali Qushji" déclare que son équipe a piraté les serveurs de LockBits et a trouvé un programme constructeur pour le ransomware LockBit 3.0.

Après que le chercheur en sécurité 3xp0rt a partagé le tweet sur la fuite du constructeur de LockBit 3.0, VX-Underground a partagé qu'ils ont été contactés le 10 septembre par un utilisateur nommé "protonleaks", qui a également partagé une copie du même programme.

VX-Underground indique que LockBitSupp, le représentant public de LockBit, affirme qu'ils n'ont pas été piratés, mais plutôt qu'un développeur mécontent a divulgué le constructeur privé du ransomware.

"Nous avons contacté le groupe Lockbit ransomware à ce sujet et avons découvert que cette fuite était un programmeur employé par le groupe Lockbit ransomware", a partagé VX-Underground dans un tweet. "Ils étaient en colère contre la direction de Lockbit et ont divulgué le constructeur".

Cette fuite n'est pas seulement un coup dur pour l'opération de ransomware LockBit, mais aussi pour les entreprises, qui connaîtront une augmentation des acteurs de la menace qui utiliseront le constructeur pour lancer leurs propres attaques.

Le constructeur se compose de quatre fichiers, un générateur de clés de chiffrement, un constructeur, un fichier de configuration modifiable et un fichier batch pour construire tous les fichiers.

Le fichier "config.json" inclus peut être utilisé pour personnaliser un crypteur, notamment en modifiant la note de rançon, en changeant les options de configuration, en décidant des processus et des services à interrompre, et même en spécifiant le serveur de commande et de contrôle auquel le crypteur enverra des données.

En modifiant le fichier de configuration, tout acteur de la menace peut l'adapter à ses propres besoins et modifier la note de rançon créée pour la relier à sa propre infrastructure.

Pour rester protégées, les organisations sont invitées à investir davantage dans des solutions de cybersécurité, en mettant l'accent sur l'utilisation optimale d'une plateforme de renseignements sur les menaces.

Source : *https://bit.ly/3CgN5TE*

Des pirates volent des comptes GitHub en utilisant de fausses notifications CircleCI

GitHub signale la présence d'une campagne d'hameçonnage qui a débuté le 16 septembre et qui cible ses utilisateurs avec des courriels usurpant l'identité de la plateforme d'intégration et de livraison continues CircleCI.

Les faux e-mails informent les destinataires que les conditions d'utilisation et la politique de confidentialité ont changé et qu'ils doivent se connecter à leur compte GitHub pour accepter les modifications et continuer à utiliser les services.

Les acteurs de la menace ont pour objectif de voler les informations d'identification des comptes GitHub et les codes d'authentification à deux facteurs (2FA) en les relayant par des proxys inversés.

Quant aux comptes protégés par des clés de sécurité matérielles pour l'authentification multifactorielle (MFA), ils ne sont pas vulnérables à cette attaque.

"Bien que GitHub lui-même n'ait pas été affecté, la campagne a eu un impact sur de nombreuses organisations victimes", informe GitHub dans un avis.

CircleCI a également publié un avis sur ses forums pour sensibiliser à la campagne malveillante, expliquant que la plateforme ne demanderait jamais aux utilisateurs de saisir des informations d'identification pour consulter les modifications apportées à ses conditions de service.

"Tout courriel provenant de CircleCI ne doit comporter que des liens vers circleci.com ou ses sous-domaines", précise l'avis de CircleCI.

Au cas où quelqu'un aurait accidentellement cliqué sur un lien dans cet e-mail, il convient de modifier immédiatement les informations d'identification de GitHub et de CircleCI, et de vérifier que les systèmes ne présentent aucune activité non autorisée.

Après avoir obtenu les informations d'identification valides du compte, les acteurs de la menace créent des jetons d'accès personnels (PAT), autorisent les applications OAuth et ajoutent parfois des clés SSH au compte pour qu'elles persistent même après une réinitialisation du mot de passe.

GitHub rapporte avoir constaté une exfiltration de contenu de dépôts privés presque immédiatement après la compromission.

Les acteurs de la menace utilisent des services VPN ou proxy pour rendre leur traçage plus difficile.

Si le compte compromis dispose d'autorisations de gestion d'organisation, les pirates créent de nouveaux comptes d'utilisateur et les ajoutent à l'organisation pour maintenir la persistance.

GitHub a suspendu les comptes pour lesquels des signes de fraude ont pu être identifiés. La plateforme a réinitialisé les mots

de passe des utilisateurs touchés, qui recevront des notifications personnalisées concernant l'incident.
La société GitHub énumère également ces contrôles de sécurité que tous les utilisateurs devraient effectuer régulièrement pour s'assurer que des pirates furtifs n'ont pas compromis leurs comptes.

Source : *https://bit.ly/3UOkM6j*

Un attaquant a pris le contrôle des serveurs Exchange

Microsoft a annoncé qu'un attaquant avait réussi à prendre le contrôle de ses serveurs Exchange en lançant des opérations de saturation d'informations d'identification grâce à des applications OAuth malveillantes sur des locataires de clouds exposés.
Cette attaque a exploité des comptes d'administrateur non sécurisés pour obtenir un accès initial à des comptes très vulnérables qui ne sont pas dotés de la fonction MFA.
Après avoir obtenu l'accès, le pirate crée une application OAuth malveillante et modifie les paramètres du serveur Exchange pour ajouter un connecteur entrant malveillant au serveur de messagerie.
Les paramètres compromis du serveur Exchange permettent de diffuser des e-mails de phishing qui incitent les destinataires à cliquer sur un lien pour recevoir un prix de valeur.
Une fois cliqué, le lien redirige les victimes vers une page de renvoi leur demandant de saisir les détails de leur carte de crédit et de s'inscrire à des abonnements payants récurrents.
Des plateformes d'envoi d'e-mails en masse couramment utilisées, telles que Amazon SES et MailChimp, ont été utilisées pour envoyer ces campagnes d'e-mails.
Afin de maintenir leur activité pendant une période prolongée, les pirates utilisent différentes mesures d'évasion de défense. Ces techniques consistent notamment à supprimer le connecteur entrant, à supprimer les modifications apportées au serveur Exchange après chaque campagne de spam, et à utiliser l'application OAuth malveillante des semaines ou des mois après son déploiement.
La campagne vise principalement les comptes de messagerie des consommateurs, mais si elle avait été utilisée pour diffuser des logiciels malveillants, les conséquences auraient pu être considérables. Ainsi, cet incident expose des failles de sécurité qui pourraient être utilisées par d'autres attaquants visant directement des organisations vulnérables.

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

GTA 6 : code source et vidéos divulgués suite au piratage de Rockstar Games

Les vidéos de gameplay et le code source de Grand Theft Auto 6 ont été divulgués à la suite de l'intrusion d'un pirate sur le serveur Slack et le wiki Confluence de Rockstar Game.
La fuite a d'abord touché le forum GTAForums, où un acteur de la menace nommé "teapotuberhacker" a partagé un lien vers une archive RAR contenant 90 vidéos volées.
Les vidéos semblent avoir été créées par des développeurs qui déboguent diverses fonctionnalités du jeu, comme les angles de caméra, le suivi des PNJ et les lieux de Vice City.
Le pirate affirme avoir récupéré "le code source et les ressources de GTA 5 et 6, ainsi que la version de test de GTA 6", mais il tente actuellement de forcer Rockstar Games à lui extorquer des fonds pour empêcher la divulgation d'autres données.
L'acteur de la menace a affirmé être à l'origine de la récente cyberattaque contre Uber et a diffusé des captures d'écran du code source de Grand Theft Auto V et Grand Theft Auto 6 comme preuve supplémentaire.
Les vidéos divulguées se sont retrouvées sur YouTube et Twitter, et Rockstar Games a émis des avis d'infraction DMCA et des demandes de retrait pour mettre les vidéos hors ligne.
Cependant, les efforts de Rockstar Game arrivent trop tard, car l'acteur menaçant et d'autres personnes avaient déjà commencé à divulguer les vidéos volées de GTA 6 et des parties du code source sur Telegram.
Par exemple, l'acteur menaçant a divulgué aujourd'hui un fichier de code source de GTA 6 de 9 500 lignes qui semble être lié à l'exécution de scripts pour diverses actions dans le jeu.
Rockstar Games a confirmé qu'ils ont subi une intrusion dans le réseau permettant aux pirates de télécharger des données de l'entreprise à partir de leurs systèmes.
"Nous avons récemment été victimes d'une intrusion dans notre réseau, au cours de laquelle un tiers non autorisé a accédé illégalement à nos systèmes et y a téléchargé des informations confidentielles, notamment des séquences de développement pour le prochain Grand Theft Auto. Pour l'instant, nous ne prévoyons pas d'interruption de nos services de jeu en direct ni d'effet à long terme sur le développement de nos projets en cours.

Nous sommes extrêmement déçus que des détails sur notre prochain jeu soient ainsi partagés avec vous tous. Notre travail sur le prochain jeu Grand Theft Auto se poursuivra comme prévu et nous sommes toujours aussi déterminés à vous offrir, à vous, nos joueurs, une expérience qui dépasse vraiment vos attentes. Nous vous tiendrons bientôt au courant et, bien sûr, nous vous présenterons ce nouveau jeu lorsqu'il sera prêt. Nous tenons à remercier tout le monde pour leur soutien continu dans cette situation." A confirmé Rockstar Games dans sa déclaration.

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

Bon à savoir

Le chargement de DLL non signées une méthode d'intégration de logiciels malveillants

Actuellement, le chargement de DLL non signées est devenu la méthode préférée pour que les acteurs de logiciels malveillants puissent évaluer leurs techniques pour échapper à la détection et exécuter des attaques plus sophistiquées.

Selon les recherches faites par Palo Alto Networks, la plupart des DLL malveillantes partagent trois caractéristiques communes :

- Les DLL sont le plus souvent écrites dans des chemins non privilégiés ;
- Les DLL ne sont pas signées ;
- Pour échapper à la détection, les DLL sont chargées par un processus signé, qu'il s'agisse d'un utilitaire dédié au chargement de DLL (tel que rundll32.exe) ou d'un exécutable qui charge des DLL dans le cadre de son activité.

Pour limiter les impacts causés par ce types d'attaques, il est conseillé de se concentrer sur les points suivants :

- Se focaliser sur l'entropie du fichier : Les binaires qui ont une valeur élevée d'entropie peuvent contenir une section emballée qui sera extraite pendant l'exécution ;
- Se concentrer sur la fréquence d'exécution : Une fréquence élevée peut indiquer une activité légitime qui se produit périodiquement, tandis qu'une fréquence faible peut être une piste pour une enquête ;
- Vérifier le chemin d'accès au fichier : Les chemins qui contiennent des dossiers ou des fichiers dont les noms sont brouillés sont plus suspects que les autres.

Dans la plupart des cas, les techniques de détection visant à bloquer les DLL malveillantes reposent sur le comportement du module après son chargement en mémoire. Ce qui peut limiter la capacité à bloquer tous les modules malveillants.

Cependant, il est possible de rechercher de manière proactive les DLL non signées malveillantes en utilisant des méthodes de chasse telles que la plateforme de détection et de réponse utilisées par les équipes de SOC.

Source : *https://bit.ly/3y2vwEu*

Evènements

Evènement du mois

NASA SPACE APPS CHALLENGE ALGERIA 2022

30 Septembre au 02 Octobre 2022

Alger, Algérie

https://nasa.microclub.net

La NASA Space Apps Challenge revient pour sa 11eme édition et pour la 6eme fois en Algérie, où le Club scientifique universitaire algérien "MICROCLUB" gère l'événement.

Cette hackathon international est sous le slogan "Make Space", il se déroulera virtuellement et en présentiel. L'événement embrasse la résolution collaborative des problèmes dans le but de produire des solutions open-source aux défis auxquels cette génération est actuellement confrontée sur Terre et dans l'espace.

Evènement à venir

DATA AND AUTOMATION SECURITY

06 Octobre 2022

Online

https://bit.ly/3SFACyj

L'intelligence artificielle peut transformer la façon dont le gouvernement saisit et utilise les données. Mais les agences fédéraux sont toujours assises sur des masses de données qui peuvent fournir une immense valeur pour aider à détecter et à contrecarrer les menaces critiques de cybersécurité. Cet événement virtuel examinera de nouvelles stratégies pour tirer parti des données dans le cadre du besoin constant et omniprésent de sécuriser rapidement les systèmes.

Cet évènement sera sponsorisé par Leidos et Women In Technology.

Référence	ANPT-2022-BV-09
Titre	Bulletin de veille N°09
Date de version	30 Septembre 2022
Contact	ssi@anpt.dz