BULLETIN DE VEILLE N°02

ANPT-2024-BV-02

« One of the main cyber-risks is to think they don't exist. The other is to try to treat all potential risks. »
- Stephane Nappo -

février 2024

Alertes de sécurité

Apple

La vulnérabilité récente des raccourcis "zéro-clic" d'Apple

23 février 2024

La faille de sécurité de haute sévérité dans l'application Raccourcis d'Apple qui pourrait permettre à un raccourci d'accéder à des informations sensibles sur l'appareil sans le consentement des utilisateurs.

La vulnérabilité, répertoriée sous le nom de CVE-2024-23204 (score CVSS : 7.5), a été corrigée par Apple le 22 janvier 2024, avec la publication de iOS 17.3, iPadOS 17.3, macOS Sonoma 14.3, et watchOS 10. 3..

"Un raccourci peut être en mesure d'utiliser des données sensibles avec certaines actions sans que l'utilisateur n'y soit invité", a déclaré le fabricant de l'iPhone dans un avis, précisant que le problème a été corrigé par des "vérifications supplémentaires des autorisations".

Apple Shortcuts est une application de script qui permet aux utilisateurs de créer des flux de travail personnalisés (ou macros) pour exécuter des tâches spécifiques sur leurs appareils. Elle est installée par défaut sur les systèmes d'exploitation iOS, iPadOS, macOS et watchOS.

La méthode consiste à sélectionner toute donnée sensible (Photos, Contacts, Fichiers et données du presse-papiers) au sein de Raccourcis, à l'importer, à la convertir à l'aide de l'option d'encodage base64 et, enfin, à la transmettre au serveur malveillant. Les données exfiltrées sont ensuite capturées et sauvegardées sous forme d'image du côté de l'attaquant à l'aide d'une application Flask, ce qui ouvre la voie à une exploitation ultérieure.

"Les raccourcis peuvent être exportés et partagés entre les utilisateurs, une pratique courante dans la communauté Shortcuts", ont déclaré les chercheurs. "Ce mécanisme de partage étend la portée potentielle de la vulnérabilité, car les utilisateurs importent à leur insu des raccourcis susceptibles d'exploiter la CVE-2024-23204." ***Source : https://bit.ly/3wyL8BM***

Microsoft

Plus de 28 500 serveurs Exchange vulnérables à un bug activement exploité

20 février 2024

Jusqu'à 97 000 serveurs Microsoft Exchange pourrait être vulnérables à une faille d'escalade des privilèges de gravité critique répertoriée sous le nom de CVE-2024-21410, que les pirates informatiques exploitent activement.

Exchange Server est largement utilisé dans les environnements professionnels pour faciliter la communication et la collaboration entre les utilisateurs, en fournissant des services de courrier électronique, de calendrier, de gestion des contacts et de gestion des tâches.

Le problème de sécurité permet à des acteurs distants non authentifiés d'effectuer des attaques par relais NTLM sur les serveurs Microsoft Exchange et augmenter leurs privilèges sur le système.

Aujourd'hui, le service de surveillance des menaces Shadowserver a annoncé que ses scanners ont identifié environ 97 000 serveurs potentiellement vulnérables.

Actuellement, il n'y a pas de preuve de concept (PoC) publiquement disponible pour la CVE-2024-21410, ce qui limite un peu le nombre d'attaquants utilisant cette faille dans leurs attaques.

Pour remédier à CVE-2024-21410, il est recommandé aux administrateurs système d'appliquer la mise à jour Cumulative Update 14 (CU14) d'Exchange Server 2019 publiée lors du Patch Tuesday de février 2024, qui active les protections de relais d'informations d'identification NTLM.

L'agence américaine de cybersécurité et de sécurité des infrastructures (CISA) a également ajouté CVE-2024-21410 à son catalogue de "vulnérabilités exploitées connues", donnant aux agences fédérales jusqu'au 7 mars 2024 pour appliquer les mises à jour/atténuations disponibles ou cesser d'utiliser le produit. ***Source : https://bit.ly/49NUHem***

Actualité

Des acteurs chinois de la menace espionnent le réseau du ministère néerlandais de la défense

Des pirates informatiques parrainés par l'État chinois se sont introduits l'année dernière dans un réseau informatique interne utilisé par le ministère néerlandais de la défense, ont déclaré les Pays-Bas mardi.

Le MIVD a déclaré avoir trouvé le logiciel malveillant sur un réseau informatique compartimenté utilisé par les forces armées du pays pour la recherche et le développement non classifiés.

Le ministre de la défense, Kajsa Ollongren, a déclaré : "Pour la première fois, le MIVD a choisi de rendre public un rapport technique sur les méthodes de travail des pirates informatiques chinois. Il est important d'attribuer ces activités d'espionnage à la Chine. De cette manière, nous augmentons la résilience internationale contre ce type de cyber-espionnage".

Selon le rapport des agences de renseignement, les pirates ont obtenu un accès initial par le biais de la vulnérabilité CVE-2022-42475, dont Fortinet avait averti en janvier qu'elle était exploitée par un "acteur avancé" pour cibler des réseaux gouvernementaux.

Après avoir accédé au réseau de la défense néerlandaise, les pirates ont déployé un cheval de Troie d'accès à distance (RAT), pour effectuer une reconnaissance du réseau informatique et exfiltrer une liste de comptes d'utilisateurs du serveur Active Directory. Software and devices."

"Bien que cet incident ait commencé par un abus de CVE-2022-42475, le logiciel malveillant COATHANGER pourrait être utilisé en combinaison avec n'importe quelle vulnérabilité logicielle présente ou future dans les dispositifs FortiGate", indique le rapport.

Peu après la divulgation de la vulnérabilité, les chercheurs ont averti qu'il y avait des centaines de milliers d'interfaces vulnérables exposées à l'internet, soit près de 70 % de toutes les installations en ligne.

L'année dernière, Christopher Glyer, du Microsoft Threat Intelligence Center, s'est demandé si la même vulnérabilité n'avait pas été utilisée dans les attaques d'un groupe de menace lié à la Chine et connu sous le nom de Volt Typhoon, qui a piraté des infrastructures critiques à Guam

Fortinet a déclaré qu'elle ne reliait pas l'exploit à Volt Typhoon "pour le moment", mais a averti qu'elle s'attendait à ce que "tous les acteurs de la menace, y compris ceux qui sont derrière la campagne Volt Typhoon, continuent d'exploiter des vulnérabilités non corrigées dans des logiciels et des appareils largement utilisés".

Source : https://bit.ly/3SZ52xl

Les attaquants de "ResumeLooters" volent des millions de dossiers professionnels

Une campagne d'attaque à grande échelle attribuée au groupe de menace ResumeLotters a été portée à la connaissance des chercheurs du Group-IB. La campagne a été active entre novembre et décembre 2023 et a été lancée avec succès contre 65 sites web pour voler plus de deux millions d'emails uniques.

Selon les chercheurs, le groupe a utilisé l'injection SQL et les attaques XSS (Cross-Site Scripting) pour cibler les sites web de recrutement et de vente au détail en Asie-Pacifique.

L'acteur de la menace a utilisé l'injection SQL pour récupérer des bases de données contenant près de 2,2 millions de lignes de données, dont plus de 500 000 représentaient des données d'utilisateurs de sites web d'emploi.

Dans certains cas, ResumeLooters a utilisé des attaques XSS pour charger des scripts malveillants sur des sites légitimes de recherche d'emploi.

Dans l'une de ses attaques XSS, le groupe a créé un faux profil d'employeur sur un site de recrutement légitime pour inciter les demandeurs d'emploi à communiquer leurs informations personnelles.

Ces attaques ont été lancées à l'aide de divers outils de test de pénétration tels que sqlmap, Acunetix, Beef Framework, X-Ray, Metasploit, ARL et Dirsearch.

Les données volées, qui comprenaient des noms, des numéros de téléphone, des dates de naissance et des informations sur les demandeurs d'emploi, ont été mises en vente sur des groupes Telegram de langue chinoise consacrés au piratage.

Plus de 70 % des victimes touchées se trouvent en Inde, à Taïwan, en Thaïlande et au Viêt Nam, suivies par quelques entreprises au Brésil, aux États-Unis, en Turquie, en Russie, au Mexique et en Italie.

Source : ***https://bit.ly/48yFw7C***

Bon à savoir

Les mots de passe plus longs ne sont pas protégés contre les tentatives intensives de piratage

On n'est jamais trop prudent en matière de sécurité des réseaux et de l'IOT. Avec un nombre rapidement croissant d'appareils

disparates connectés aux infrastructures d'entreprise et industrielles, mieux vaut prévenir que guérir.
Pour les administrateurs réseau, il ne s'agit plus seulement de protéger les ordinateurs portables et les PC, mais plutôt de gérer un réseau composé d'une palette colorée de matériel connecté, y compris des appareils mobiles et des appareils IoT à faible coût. Mais comment pouvez-vous assurer la sécurité de votre réseau lorsque chaque appareil suit ses propres règles ? La réponse est (relativement) simple : NE FAIRE CONFIANCE À PERSONNE !
C'est là qu'intervient le concept d'"architecture zéro confiance", qui est un concept de sécurité basé sur le fait de ne pas faire confiance à un appareil par défaut simplement parce qu'il fait partie de votre réseau. Au lieu de cela, chaque appareil doit s'authentifier pour chaque connexion qu'il souhaite établir. Étant donné que toute connexion possible implique au moins deux parties, l'authentification requise ici est appelée authentification mutuelle.
Il existe différents protocoles de communication qui utilisent l'authentification mutuelle, tels que SSH et TLS. Ce que ces protocoles ont en commun, c'est que l'authentification est basée sur des certificats d'appareil uniques. Sans ce certificat, un appareil ne peut pas s'authentifier.
La base d'une architecture de confiance zéro est établie en choisissant la bonne façon de fournir à l'appareil les clés qui sont à la base de son certificat unique. La méthode choisie variera en fonction du matériel de chaque appareil.
Les différentes approches offrent différents niveaux de sécurité, mais elles ont toutes en commun le fait qu'elles doivent instiller le niveau de confiance approprié pour que la clé privée reste privée. Lorsqu'un appareil est équipé d'une paire de clés publique-privée, une autorité de certification peut fournir la pièce suivante du puzzle en générant un certificat pour l'appareil. Une fois qu'un appareil dispose de ce certificat unique, il est prêt pour l'authentification mutuelle qui est nécessaire pour être autorisé à entrer en toute sécurité dans un réseau construit sur une architecture de confiance zéro.

Source : ***https://bit.ly/49NhCqb***

Evènements

Evènement du mois

Algeria cyber forum – La 8eme Edition

21-22 Février 2024 – club des pain Alger

https://bit.ly/4bNT1n7

Le World Trade Center Algiers vous invite à la 8ème édition « Algeria Cyber Forum ». Un rendez-vous incontournable des experts de la cybersécurité qui se tiendra les 21 & 22 Février 2023 au CIC – Alger. Plus qu'un événement, cette édition se veut être une véritable plateforme d'échanges qui accompagne tous les acteurs publics et privés du marché pour faire face aux cybermenaces auxquelles ils sont exposés dans leur transformation numérique et intégration des nouvelles technologies dans leurs stratégies de développement.

.

Evènement à venir

La cybersécurité pour les experts des propriété - Êtes-vous en sécurité ? 2024

5 mars 2024 - Online

https://bit.ly/3Ih1rpi

Cette formation de 3,5 heures sur la cybersécurité s'adresse aux propriétaires de sociétés immobilières, en particulier à ceux qui traitent des transactions de grande valeur. Au cours de cette formation, vous acquerrez les connaissances et les compétences nécessaires pour protéger votre entreprise et les données de vos clients dans le paysage de plus en plus numérique des transactions immobilières. Différents sujets à explorer comme les cybermenaces, la protection des données, la communication sécurisée, la protection contre phishing...etc.

Référence	ANPT-2024-BV-02
Titre	Bulletin de veille N°02
Date de version	28 février 2024
Contact	ssi@anpt.dz