BULLETIN DE VEILLE N°04

ANPT-2024-BV-04

« 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 -

Avril 2024

Alertes de sécurité

Windows

Rust trouve un correctif pour le bug d'injection de commande critique sous Windows dans la librairie std

10 avril 2024

Les programmeurs sont invités à mettre à jour leurs versions de Rust après que les experts en sécurité ont corrigé une vulnérabilité critique qui pourrait conduire à des injections de commandes malveillantes sur les machines Windows.

La vulnérabilité, qui porte un score de gravité CVSS parfait de 10 sur 10, est répertoriée sous le nom de CVE-2024-24576. Elle affecte la bibliothèque standard Rust, qui n'échappe pas correctement aux arguments lors de l'invocation de fichiers batch sur Windows à l'aide de l'API Command de la bibliothèque - en particulier, std::process::Command.

"Un attaquant capable de contrôler les arguments transmis au processus créé pourrait exécuter des commandes shell arbitraires en contournant l'échappement", a déclaré Pietro Albini du Rust Security Response Working Group, qui a rédigé l'avis. Le principal problème semble provenir du programme CMD.exe de Windows, qui a des règles d'analyse plus complexes, et Windows ne peut pas exécuter de fichiers batch sans lui, selon le chercheur de Flatt Security, basé à Tokyo, qui a signalé le problème.

Selon M. Albini, l'invite de commande de Windows possède sa propre logique de séparation des arguments, qui fonctionne différemment des API Command::arg et Command::args fournies par la bibliothèque standard, qui permettent généralement de transmettre en toute sécurité des données d'entrée non fiables aux processus créés.

Chris Denton, un contributeur à la bibliothèque std de Rust, a développé le correctif qui a permis d'atténuer le problème, en améliorant le code d'échappement et en s'assurant que l'API de commande renvoie une erreur InvalidInput lorsqu'elle ne peut pas échapper les arguments en toute sécurité.

Rust a publié la version 1.77.2 mardi, indiquant que toutes les versions précédentes étaient vulnérables.

Source : https://bit.ly/3xO9sQF

WordPress

Le CERT japonais signale une vulnérabilité critique dans le plugin WordPress Forminator

22 avril 2024

Le CERT japonais signale une vulnérabilité dans le plugin WordPress Forminator qui permet le téléchargement illimité de fichiers sur le serveur. Le CERT du Japon a averti que le plugin WordPress Forminator, est affecté par de multiples vulnérabilités, y compris une faille qui permet des téléchargements de fichiers non restreints vers le serveur.

Forminator est un plugin WordPress populaire qui permet aux utilisateurs de créer facilement divers formulaires pour leur site web sans avoir besoin de connaissances en codage. Le plugin est installé dans plus de 500 000 sites web.

L'une de ces vulnérabilités est un problème critique, répertorié sous le nom de CVE-2024-28890 (CVSS v3 : 9.8), qu'un attaquant distant peut exploiter pour télécharger du code malveillant sur des sites WordPress utilisant le plugin.

« Un attaquant distant peut obtenir des informations sensibles en accédant à des fichiers sur le serveur, modifier le site qui utilise le plugin et provoquer un déni de service (CVE-2024-28890) », peut-on lire dans le bulletin de sécurité publié par le JPCERT.

Le bulletin met également en garde contre les vulnérabilités CVE-2024-31077 (CVSS score 7.2) - Faille d'injection SQL et CVE-2024-31857 (CVSS score 6.1) - Faille de script cross.

Les versions 1.29.3 de Forminator ont corrigé toutes les vulnérabilités, il est recommandé aux administrateurs de mettre à jour leurs installations dès que possible. Selon les statistiques fournies par WordPress.org, le plugin compte plus de 500 000 installations actives, mais seulement 55,9 % (plus de 279) utilisent la version 1.29, cela signifie que plus de 200 000 sites sont vulnérables aux cyberattaques.

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

Actualité

Des pirates nord-coréens ciblent des dizaines d'entreprises du secteur de la défense

La police sud-coréenne a révélé l'existence d'une vaste campagne de piratage informatique au cours de laquelle des secrets de défense ont été dérobés par des pirates du Nord sur une période d'un an.

Un rapport de l'Agence nationale de la police coréenne (KNPA) publié hier attribue cette campagne à trois groupes soutenus par l'État nord-coréen : Lazarus, Kimsuky et Andariel

Selon des rapports locaux, ces groupes auraient ciblé 83 entreprises de défense et sous-traitants, et seraient parvenus à dérober des informations sensibles à 10 d'entre eux entre octobre 2022 et juillet 2023, bien que la campagne ait duré plus d'un an.

La KPNA a révélé que certaines des entreprises en question n'étaient « absolument pas au courant » qu'elles avaient été victimes d'une intrusion, lorsqu'elles ont été contactées par la police.

Pour en savoir plus sur les cyber-attaques nord-coréennes : Des attaquants nord-coréens exploitent une vulnérabilité critique de CI/CD

Dans un cas révélé par le rapport de la KPNA, les auteurs de la menace ont exploité une vulnérabilité dans un système de messagerie électronique qui leur permettait de télécharger de gros fichiers sans authentification.

Dans un autre cas, ils ont profité d'une mauvaise sécurité des mots de passe pour détourner le compte d'une société tierce de maintenance informatique et infecter ainsi un sous-traitant de la défense avec des logiciels malveillants. L'employé dont le compte a été piraté aurait utilisé le même mot de passe pour son courrier électronique privé et celui de l'entreprise.

Dans un autre cas, ils ont profité d'une mauvaise sécurité des mots de passe pour détourner le compte d'une société tierce de maintenance informatique et infecter ainsi un sous-traitant de la défense avec des logiciels malveillants. L'employé dont le compte a été piraté aurait utilisé le même mot de passe pour son courrier électronique privé et celui de l'entreprise. Dans un troisième exemple cité par la KPNA, les administrateurs ont interrompu les contrôles de sécurité sur un réseau interne pendant les tests, ce qui a permis à leurs adversaires de compromettre et d'exfiltrer des données sensibles.

La Corée du Sud est devenue un acteur de plus en plus important dans le commerce mondial des armes, signant ces dernières années des contrats d'une valeur de plusieurs milliards de dollars pour la vente d'obusiers, de chars et d'avions de chasse, selon Reuters.

Source https://bit.ly/3WklED7

Le comté du Missouri déclare l'état d'urgence en raison d'une attaque présumée de ransomware

Le comté de Jackson, Missouri, dans l'Etats-Unis a déclaré l'état d'urgence et fermé ses principaux bureaux pour une durée indéterminée afin de répondre à ce que les autorités estiment être une attaque par ransomware qui a rendu certains de ses systèmes informatiques inopérants.

"Le comté de Jackson a identifié d'importantes perturbations dans ses systèmes informatiques, potentiellement attribuables à une attaque de ransomware", ont écrit les autorités mardi. "Les premières indications suggèrent des incohérences opérationnelles dans son infrastructure numérique et certains systèmes ont été rendus inopérants alors que d'autres continuent à fonctionner normalement."

Les systèmes confirmés inopérants comprennent le paiement des impôts et des propriétés en ligne, la délivrance de licences de mariage et la recherche de détenus. En conséquence, les bureaux d'évaluation, de recouvrement et d'enregistrement des actes dans tous les sites du comté sont fermés jusqu'à nouvel ordre.

La fermeture a eu lieu le jour même où le comté organisait une élection spéciale pour voter sur une proposition de taxe de vente destinée à financer un stade pour les Kansas City Royals de la MLB et les Kansas City Chiefs de la NFL. Ni le bureau électoral du comté de Jackson ni celui de Kansas City n'ont été touchés par l'attaque ; ils restent tous deux ouverts.

Selon Brett Callow, analyste des menaces pour la société de sécurité Emsisoft, 28 comtés, municipalités ou gouvernements tribaux ont été touchés par des attaques de ransomware cette année. L'année dernière, il y en a eu 95 et 106 en 2022.

Source : https://bit.ly/3w81ktP

Bon à savoir

Des pirates attaquent les équipes Infra avec de fausses publicités pour PuTTY et FileZilla

Une campagne sophistiquée de publicité malveillante cible les administrateurs de systèmes du monde entier. Les attaquants utilisent de fausses publicités pour des utilitaires systèmes populaires afin de distribuer une dangereuse souche de logiciel malveillant connue sous le nom de Nitrogen.

La campagne exploite la confiance que les utilisateurs accordent aux publicités des moteurs de recherche. En affichant des résultats de recherche sponsorisés pour des utilitaires tels que PuTTY et FileZilla, les attaquants peuvent attirer leurs victimes. Une fois cliquées, ces publicités malveillantes conduisent les utilisateurs à télécharger ce qu'ils croient être des installateurs de logiciels légitimes. Cependant, ces installateurs sont des versions trojanisées conçues pour infecter le système de l'utilisateur avec le logiciel malveillant Nitrogen.

Ce logiciel malveillant sert de passerelle aux attaquants pour obtenir un accès initial aux réseaux privés, qui peuvent ensuite être exploités pour voler des données ou pour déployer des ransomwares tels que BlackCat/ALPHV.

Malgré les rapports adressés à Google, les publicités malveillantes continuent d'être diffusées, ce qui a incité la communauté de la cybersécurité à partager des informations détaillées sur les tactiques, techniques et procédures (TTP) utilisées par les attaquants et les indicateurs de compromission (IOC) afin d'aider les administrateurs de systèmes à se défendre contre ces menaces.

Pour lutter contre cette menace, la société de cybersécurité ThreatDown a bloqué ces sites web malveillants et empêché les utilisateurs d'être incités à télécharger des logiciels malveillants.

La prévalence de la publicité malveillante en tant que vecteur de cyberattaques a mis en évidence la nécessité d'une meilleure formation des utilisateurs, spécialement conçue pour reconnaître et éviter de telles menaces.

Si la formation au phishing pour les menaces liées au courrier électronique est bien connue, une formation similaire pour la publicité malveillante n'est pas encore très répandue.

Pour protéger les terminaux contre les publicités malveillantes, des stratégies de groupe peuvent être mises en œuvre pour restreindre le trafic provenant de réseaux publicitaires importants ou moins connus.

Source* : *https://bit.ly/44i7vIA

Evènements

Evènement du mois

CSA 2024 : La 6ème Conférence sur les systèmes informatiques et applications

21-23 avril - club des pain Alger

https://bit.ly/4d9tYeF

L'Ecole Militaire Polytechnique - Chahid Abderrahmane Taleb (EMP) organise la sixième édition de la conférence Computing Systems and Applications (CSA) qui aura lieu du 23 au 24 avril 2024. La conférence est ouverte aux chercheurs, universitaires et professionnels de l'industrie intéressés par les dernières avancées scientifiques et technologiques dans différents domaines de l'informatique. La CSA sera un lieu privilégié permettant aux étudiants, aux chercheurs, aux universitaires et aux industriels de partager leurs nouvelles idées.

Evènement à venir

CTOFORUM Algeria

20-22 MAI 2024 - palais de la culture Moufdi Zakaria

https://bit.ly/4b5btH7

CTO FORUM est le rendez-vous des plus grands acteurs du secteur IT. Ce forum a vocation d'être la Vitrine, par excellence, des technologies les plus innovantes mises à disposition des entreprises et des professionnels du secteur, dont l'objectif est de privilégier le B2B entre top décideurs et exposants.

CTO Forum est également le rendez-vous des dirigeants des entreprises publiques et privées qui y viennent pour s'informer et échanger sur les dernières nouveautés, ainsi que sur les grandes tendances du marché qui offre, périodiquement, de nouveaux équipements et de nouvelles solutions IT.

Référence	ANPT-2024-BV-02
Titre	Bulletin de veille N°02
Date de version	30 avril 2024
Contact	ssi@anpt.dz