« La cyber-sécurité est bien plus qu'une affaire d'informatique.»
- Kirsten Manthorne-

BULLETIN DE VEILLE N°05

ANPT-2025-BV-05

Juin 2025

Alertes de sécurité

Windows

Une nouvelle vulnérabilité de Windows RDP permet des attaques en réseau

14 Mai 2025

Microsoft a récemment divulgué deux vulnérabilités critiques affectant les services Remote Desktop Protocol (RDP) et Remote Desktop Gateway (RD Gateway) de Windows, identifiées comme CVE-2025-29966 et CVE-2025-29967. Ces failles, de type dépassement de tampon sur le tas, permettent à des attaquants non authentifiés d'exécuter du code arbitraire à distance en envoyant des paquets spécialement conçus aux systèmes vulnérables. Les deux vulnérabilités présentent un score CVSS v3.1 de 8.8, soulignant leur gravité potentielle.

La vulnérabilité CVE-2025-29966 cible spécifiquement le service RDP de Windows, qui facilite la connectivité à distance aux machines physiques et virtuelles. Quant à CVE-2025-29967, elle affecte le service RD Gateway, responsable de l'authentification et de la gestion des connexions RDP pour les utilisateurs externes. L'exploitation réussie de ces failles pourrait accorder aux attaquants des privilèges au niveau système sans nécessiter d'interaction de l'utilisateur.

Bien qu'aucune exploitation active n'ait été signalée au moment de la divulgation, Microsoft a publié des mises à jour de sécurité dans le cadre de son cycle de correctifs de mai 2025 pour remédier à ces vulnérabilités. Les organisations sont fortement encouragées à appliquer ces correctifs immédiatement, en particulier pour les systèmes exposés à Internet. Des mesures supplémentaires incluent la restriction de l'accès RDP via la segmentation du réseau et des règles de pare-feu, l'activation de l'authentification au niveau du réseau (NLA) et la surveillance des activités RDP suspectes.

Ces vulnérabilités rappellent l'importance de sécuriser les infrastructures d'accès à distance, surtout dans un contexte de travail hybride croissant. La mise en œuvre rapide des correctifs, combinée à des pratiques de sécurité robustes, est essentielle pour prévenir les attaques potentielles exploitant ces failles.

Source : https://bit.ly/3ZfW4zL

Node.js

La vulnérabilité de Node.js permet aux attaquants de bloquer des processus et d'interrompre des services

15 Mai 2025

Une vulnérabilité critique, identifiée comme CVE-2025-23166, a été découverte dans Node.js, affectant les versions 4.0 à 20.19.1, 22 à 22.15.0 et 24 à 24.0.1. Cette faille provient d'une mauvaise gestion des erreurs dans les opérations cryptographiques asynchrones, en particulier dans la méthode C++ SignTraits::DeriveBits(). Lorsqu'elle traite des entrées non fiables dans des threads en arrière-plan, cette méthode peut appeler incorrectement ThrowException(), entraînant un plantage du processus Node.js. Ce bug permet à un attaquant distant de provoquer une attaque par déni de service (DoS), rendant les applications inaccessibles.

Le projet Node.js a publié des correctifs de sécurité le 14 mai 2025, disponibles dans les versions 20.19.2 (LTS), 22.15.1 (LTS), 23.11.1 (courante) et 24.0.2 (courante). Ces mises à jour corrigent également d'autres failles, telles que CVE-2025-23167, liée à l'analyse des en-têtes HTTP, et CVE-2025-23165, concernant certaines opérations système.

Les organisations utilisant des versions affectées doivent appliquer rapidement ces correctifs pour éviter des interruptions ou compromissions. Il est également recommandé de revoir la gestion des entrées non fiables dans les opérations cryptographiques et de mettre en œuvre des mécanismes de gestion des erreurs appropriés. Pour les environnements utilisant des versions non supportées, une mise à niveau vers une version maintenue ou l'utilisation d'un support étendu est conseillée.

Enfin, il est essentiel de suivre les avis de sécurité officiels et de maintenir ses dépendances à jour. L'adoption de bonnes pratiques de développement, notamment en matière de gestion des erreurs, contribue à réduire les surfaces d'attaque. La vigilance face à ce type de vulnérabilité permet de renforcer la sécurité des applications Node.js et de limiter les risques liés à des attaques distantes.

Source : https://bit.ly/4dItYTAF

Actualité

Le registre d'état de la pologne temporairement bloqué à la suite d'un cyberincident

Le 30 avril 2025, la Pologne a été confrontée à une cyberattaque majeure qui a temporairement paralysé ses registres d'État, notamment le système PESEL – la base de données centrale contenant les informations personnelles des citoyens et résidents étrangers. Cette attaque a perturbé l'accès à des services gouvernementaux essentiels, tels que l'application mObywatel et les plateformes de déclaration fiscale en ligne. L'incident est survenu à un moment critique, coïncidant avec la date limite de déclaration des impôts en Pologne.

Le ministère du Numérique a confirmé la perturbation sans en préciser la cause exacte, assurant toutefois qu'aucune donnée sensible n'avait été compromise. Selon les médias locaux, il s'agirait d'une attaque par déni de service distribué (DDoS), où les systèmes sont submergés par un trafic fictif pour les rendre inaccessibles. L'identité des auteurs reste inconnue. Le ministre des Affaires numériques, Krzysztof Gawkowski, a souligné que la Pologne est l'une des cibles les plus fréquentes de cyberattaques, souvent attribuées à des acteurs russes.

Cette attaque s'inscrit dans une série d'incidents similaires en Europe de l'Est. En décembre, des hackers présumés russes ont compromis l'infrastructure des registres ukrainiens, paralysant les services pendant des semaines. En janvier, le registre foncier de la Slovaquie a été la cible de ce que les autorités ont qualifié de cyberattaque la plus grave de l'histoire du pays. Même la Russie a vu son agence gouvernementale Rosreestr, chargée des enregistrements fonciers, être infiltrée par des hackers non identifiés.

Face à ces menaces croissantes, la Pologne a investi 760 millions de dollars dans la cybersécurité en juin dernier. Le gouvernement encourage les citoyens à bloquer leur numéro PESEL via l'application mObywatel ou en ligne pour prévenir toute utilisation frauduleuse. Il est également recommandé de surveiller régulièrement les activités liées à son identité et de signaler toute activité suspecte aux autorités compétentes.

Source : ***https://bit.ly/45CMuL7***

Un acteur malveillant menaçant vend 1,2 milliard d'enregistrements Facebook

Un acteur malveillant, connu sous le pseudonyme ByteBreaker, prétend avoir collecté 1,2 milliard de profils Facebook en abusant d'une API de la plateforme.

Il propose cette base de données à la vente sur un forum spécialisé dans les violations de données. Un échantillon de 100 000 utilisateurs partagé sur le forum comprend des informations telles que le nom complet, le pseudo, la date de naissance, le numéro de téléphone, l'adresse e-mail, le genre, l'identifiant unique (UID) et la localisation (ville, État, pays). ByteBreaker affirme que cette base est inédite et n'a jamais été divulguée auparavant.

Cependant, des experts en cybersécurité, notamment de Hackread, soulignent des incohérences dans les affirmations de ByteBreaker. Bien que l'échantillon de données semble authentique, certaines informations correspondent à des données déjà divulguées lors de la fuite de 2021, qui avait exposé les informations de plus de 500 millions d'utilisateurs. De plus, ByteBreaker avait précédemment proposé une base de 780 millions de profils, utilisant le même échantillon de données. Ces éléments suggèrent que la base actuelle pourrait être une compilation de données antérieures, plutôt qu'une nouvelle fuite.

Une autre anomalie réside dans la structure des données. ByteBreaker mentionne que la base contient 1,2 milliard de profils, mais indique également que le fichier comporte 200 millions de lignes, chaque ligne représentant un utilisateur unique. Cette contradiction soulève des doutes sur la véracité de la taille réelle de la base. De plus, les informations de contact de ByteBreaker sur Telegram varient entre les différentes annonces, ce qui ajoute à la confusion.

Face à ces incertitudes, il est recommandé aux utilisateurs de Facebook de rester vigilants. Même si cette fuite s'avère être une réutilisation de données anciennes, les informations personnelles restent sensibles et peuvent être exploitées à des fins malveillantes. Il est conseillé de renforcer la sécurité de ses comptes, de surveiller les activités suspectes et de se tenir informé des évolutions concernant cette affaire.

Source : https://bit.ly/4mINbsr

Bon à savoir

Les types de hackers : white hat, black hat, grey hat

Dans le monde de la cybersécurité, le terme "hacker" ne désigne pas uniquement un cybercriminel. Il englobe différents profils, classés selon leurs intentions et la légalité de leurs actions. On distingue principalement trois types de hackers : les white hats, les black hats et les grey hats. Ces catégories permettent de mieux comprendre les motivations derrière les attaques informatiques et les pratiques de sécurité utilisées dans l'univers numérique.

Les white hats (ou "hackers éthiques") sont des experts en sécurité informatique qui utilisent leurs compétences pour le bien. Travaillant souvent pour des entreprises ou des gouvernements, ils testent les systèmes, identifient les vulnérabilités et proposent des solutions pour renforcer la sécurité. Ils agissent toujours avec l'autorisation des propriétaires des systèmes, dans un cadre légal. Leur objectif est de prévenir les attaques et de protéger les données. Ils jouent un rôle crucial dans les tests d'intrusion, les audits de sécurité et le développement de politiques de cybersécurité.

À l'opposé, les black hats sont les pirates malveillants. Ils exploitent les failles de sécurité pour voler des données, détruire des systèmes, installer des malwares ou tirer profit d'attaques comme les ransomwares. Leurs actions sont illégales et motivées par le gain financier, la vengeance ou l'idéologie.

Entre les deux se trouvent les grey hats, qui naviguent dans une zone grise. Ils peuvent pénétrer un système sans autorisation, mais sans intention malveillante. Parfois, ils alertent l'entreprise concernée sur les failles découvertes, mais leurs méthodes restent discutables d'un point de vue légal. Ces trois profils illustrent les multiples facettes du hacking dans l'univers numérique.

Evènements

Evènement à venir

Sécurité de l'information et gestion des données
Cours 2025

02 - 06 Juin 2025 - Online

https://bit.ly/4hfzMVL

L'événement Le Information Security and Data Management Course 2025 est un atelier en ligne de cinq jours, prévu du 2 au 6 juin 2025, organisé par le Foscore Development Center. Cet événement vise à renforcer les compétences des professionnels en matière de sécurité de l'information et de gestion des données, en mettant l'accent sur les meilleures pratiques et les stratégies actuelles pour protéger les systèmes d'information.

Classé parmi les 100 meilleurs événements en ligne dans le domaine de la sécurité et de la défense, ce cours attire des participants du monde entier, notamment des étudiants, des ingénieurs, des directeurs et des analystes en cybersécurité. Les sessions se dérouleront de **9h00 à 18h00** (heure locale), offrant une immersion complète dans les thématiques abordées.

Référence	ANPT-2025-BV-05
Titre	Bulletin de veille N°05
Date de version	31 Mai 2025
Contact	ssi@anpt.dz