« 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 -

BULLETIN DE VEILLE N°03

ANPT-2025-BV-03

Mars 2025

Alertes de sécurité

Open AI

Les cybercriminels exploitent la vulnérabilité de ChatGPT d'OpenAI dans des attaques actives

18 Mars 2025

Une vulnérabilité SSRF (server-side request forgery) récemment révélée, répertoriée sous le nom de CVE-2024-27564, est devenue une cible importante pour les cybercriminels, avec plus de 10 479 tentatives d'attaques enregistrées à partir d'une seule IP malveillante, selon les dernières recherches de Veriti. La faille, qui affecte l'infrastructure ChatGPT d'OpenAI, permet aux attaquants d'injecter des URL malveillantes dans les paramètres d'entrée, forçant ainsi l'application à effectuer des requêtes involontaires en leur nom.

Bien qu'il s'agisse d'un problème de gravité moyenne, les conclusions de Veriti révèlent que 35 % des entreprises ne sont pas protégées en raison d'une mauvaise configuration de leurs systèmes de prévention des intrusions (IPS), de leur pare-feu pour applications Web (WAF) et de leurs paramètres généraux de pare-feu. Le rapport souligne une réalité cruciale en matière de cybersécurité : « Aucune vulnérabilité n'est trop petite pour être prise en compte, les attaquants exploiteront toutes les faiblesses qu'ils pourront trouver. »

L'impact réel de cette vulnérabilité se fait déjà sentir dans de nombreux secteurs, les institutions financières apparaissant comme des cibles de choix en raison de leur dépendance à l'égard des services pilotés par l'IA et des intégrations d'API.

« Ignorer les vulnérabilités de gravité moyenne est une erreur coûteuse, en particulier pour les organisations financières de grande valeur », avertit le rapport de Veriti.

Si les institutions financières restent une cible privilégiée pour les attaquants, les organisations gouvernementales américaines figurent également parmi les secteurs les plus ciblés. Plus de 10000 tentatives d'attaques ont été détectées en une semaine seulement, ce qui souligne l'ampleur et l'intensité de la menace.

Les équipes de sécurité doivent réviser leurs configurations de sécurité, surveiller les activités malveillantes et prioriser la sécurité de l'IA pour limiter les risques liés à la vulnérabilité CVE-2024-27564. Il est crucial de protéger les systèmes contre les attaques et de résoudre les lacunes de sécurité liées à l'IA et aux API.

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

Wordpress

Le plugin WordPress CVE-2025-2563 obtient un score de 9,8 et menace des milliers de sites d'adhésion

27 Mars 2025

Une vulnérabilité critique a été découverte dans le plugin "User Registration & Membership" de WordPress, utilisé pour gérer les utilisateurs et les adhésions sur des sites. Cette faille, identifiée sous le nom de CVE-2025-2563, a obtenu un score CVSS de 9,8, ce qui indique une menace élevée. Le plugin est utilisé sur plus de 60 000 sites WordPress actifs, ce qui en fait une cible de choix pour les cybercriminels. Le problème réside dans la fonction "prepare_members_data()", où une mauvaise gestion des rôles d'utilisateur permet à un attaquant non authentifié de créer des comptes utilisateurs avec des privilèges d'administrateur, leur permettant ainsi de prendre le contrôle complet du site.

Cela expose les sites affectés à des risques importants, car un attaquant peut alors modifier ou supprimer du contenu, voler des données sensibles ou installer des logiciels malveillants. L'élévation des privilèges est particulièrement dangereuse dans ce cas, car elle donne à l'attaquant un accès complet sans nécessiter d'authentification préalable. Les versions du plugin concernées vont de la version 1.0 à la version 4.1.1 incluse. En réponse à cette vulnérabilité, les développeurs ont rapidement publié une mise à jour corrective, la version 4.1.2, qui corrige le problème de gestion des rôles et empêche la création de comptes administrateur non autorisés.

Les administrateurs de sites utilisant ce plugin sont fortement conseillés de mettre à jour vers la version 4.1.2 pour se protéger contre cette vulnérabilité. La mise à jour permet de limiter les risques d'attaques et de sécuriser les données des utilisateurs. Cette situation met en lumière l'importance de maintenir à jour les plugins WordPress et de surveiller les alertes de sécurité. Une réponse rapide aux vulnérabilités est cruciale pour garantir la sécurité des sites Web et protéger les informations sensibles des utilisateurs.

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

Actualité

La Russie affirme que l'Ukraine a piraté des organisations nationales de jeunesse pour recruter des mineurs

La Russie a accusé le renseignement militaire ukrainien, avec le soutien présumé de l'OTAN, d'avoir piraté deux organisations de jeunesse soutenues par le Kremlin, Avangard et Yunarmiya. Selon le Service fédéral de sécurité (FSB), des opérateurs ukrainiens ont accédé à des comptes de messagerie et modifié des fichiers, recueillant des informations sur des mineurs susceptibles d'être utilisées pour des opérations d'espionnage et de sabotage. Le FSB a précisé que les fichiers modifiés avaient été "distribués aux écoles de Moscou", exposant ainsi les jeunes à un recrutement potentiel pour des activités anti-russes. L'attaque ferait partie d'une campagne de cyberattaques plus large visant à saper les efforts de la Russie, en particulier ceux des organisations axées sur l'éducation militaire et patriotique des enfants et des jeunes.

Avangard, l'une des organisations touchées, a démenti les accusations, affirmant qu'aucune donnée n'avait été compromise. Le directeur du groupe a spécifiquement rejeté les affirmations selon lesquelles les comptes de messagerie ou les fichiers avaient été piratés, insistant sur le fait que leurs systèmes étaient sécurisés. Malgré ce démenti, les autorités russes ont qualifié l'incident de violation grave, affirmant que des opérateurs ukrainiens, avec l'aide de l'OTAN, tentaient de s'infiltrer dans les organisations pour perturber les efforts de la Russie visant à endoctriner et recruter des mineurs. Le mouvement Yunarmiya, également ciblé par le piratage, implique une formation militaire pour les jeunes et a déjà été confronté à des cyberattaques similaires dans le passé.

Cet incident de piratage s'inscrit dans une série de cyberattaques entre les deux belligérants dans le conflit en cours entre la Russie et l'Ukraine, où la guerre numérique est devenue une partie intégrante de la stratégie militaire. Les accusations du FSB contre l'Ukraine font partie d'une guerre de l'information plus large entre les deux nations, chacune utilisant des tactiques numériques pour affaiblir l'influence de l'autre. Bien que les accusations n'aient pas été vérifiées de manière indépendante, elles mettent en lumière le rôle de plus en plus sophistiqué des opérations cybernétiques dans les conflits modernes, où "la désinformation et l'espionnage numérique sont souvent utilisés comme outils de guerre".

Source : ***https://bit.ly/414hEbT***

Plus de 4 000 adresses IP de fournisseurs d'accès à Internet ciblées par des attaques sophistiquées visant à déployer des voleurs d'informations et des cryptomineurs

L'échange Un récent rapport a révélé que plus de 4 000 adresses IP d'ISP en Chine et sur la côte ouest des États-Unis ont été ciblées dans le cadre d'une campagne d'exploitation à grande échelle. Cette campagne est attribuée à un acteur malveillant utilisant des attaques par force brute pour exploiter des identifiants faibles et déployer des malwares sur les systèmes compromis. Les outils malveillants déployés incluent principalement des voleurs d'informations et des mineurs de cryptomonnaies, qui exploitent les machines victimes pour des tâches lourdes, comme le minage de cryptomonnaie XMRig. De plus, les attaques incluent la livraison de binaires conçus pour l'exfiltration de données et pour maintenir la persistance dans les réseaux ciblés.

Les acteurs malveillants s'appuient sur des langages de script comme Python et PowerShell, ce qui leur permet d'exécuter des opérations dans des environnements restreints. Une fois l'accès initial acquis, l'attaque effectue un balayage du réseau et installe des fichiers exécutables qui facilitent à la fois le vol d'informations et le minage de cryptomonnaie Monero. L'une des caractéristiques des voleurs d'informations est leur capacité à capturer des captures d'écran et à extraire le contenu du presse-papiers, ciblant spécifiquement les adresses de portefeuilles de cryptomonnaies telles que Bitcoin, Ethereum et d'autres.

Les attaques utilisent un outil de scan massif pour sonder de grandes quantités d'adresses IP à la recherche de ports ouverts, qui sont ensuite exploités pour des tentatives de connexion par force brute. Cette méthode permet aux attaquants de contourner les mesures de sécurité et de compromettre les réseaux afin de voler des informations sensibles et d'exploiter les ressources des systèmes à des fins financières. Ces découvertes soulignent la sophistication croissante des cybercriminels ciblant l'infrastructure essentielle des ISP à travers différentes régions, mettant en évidence l'importance de mesures de sécurité robustes pour prévenir de telles intrusions.

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

Bon à savoir

1 entreprise sur 8 a été victime d'une faille due aux médias sociaux

Les réseaux sociaux, tels que Facebook, LinkedIn et Twitter, sont devenus des armes cybernétiques privilégiées pour les criminels. En raison de la quantité massive de données qu'ils contiennent et de leur portée mondiale, ces plateformes sont devenues un terrain de jeu idéal pour les cyberattaques. Les statistiques montrent une augmentation des incidents liés aux réseaux sociaux, avec des entreprises souffrant de violations de données liées à des attaques via ces canaux. Les escroqueries et les attaques de phishing, souvent déguisées en communications légitimes, sont des exemples de l'exploitation de ces plateformes par les cybercriminels pour manipuler les utilisateurs et exécuter des attaques à grande échelle.

Ces menaces ne sont pas nouvelles, mais les réseaux sociaux amplifient leur portée, augmentant ainsi le risque pour les entreprises. En effet, des informations disponibles sur des plateformes comme LinkedIn ont été utilisées pour des attaques de reconnaissance,

comme lors de la violation de données d'Anthem Health en 2015, qui a vu 80 millions de dossiers volés. De même, Twitter a été utilisé pour diffuser un exploit de malware sophistiqué, preuve que les réseaux sociaux ne sont plus uniquement des outils de communication, mais des vecteurs potentiels de cyberattaques.

Face à cette menace grandissante, il est crucial que les entreprises traitent les réseaux sociaux comme une menace de cybersécurité sérieuse. Cela implique de mettre en place des stratégies de sécurité adaptées, de surveiller activement les canaux sociaux pour détecter toute anomalie et d'adopter une approche proactive vis-à-vis des menaces externes, telles que les usurpations d'identité ou les tentatives de doxing. Les entreprises doivent également s'assurer de coordonner leurs efforts de sécurité avec les parties prenantes internes, telles que les équipes juridiques et de conformité, pour couvrir tous les aspects de la sécurité des réseaux sociaux.

Evènements

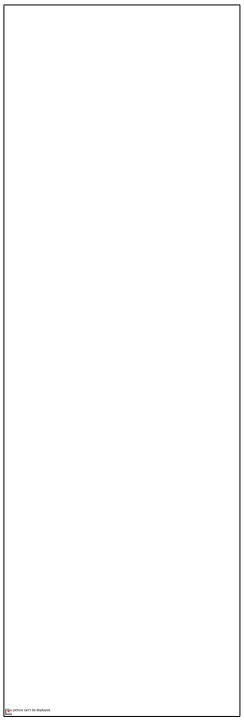
Evènement à venir

ICT Africa Summit 2025 : Unlocking Digital Horizons

21-23 Avril 2025

Palais des Expositions, Pavillon A, SAFEX, Alger, Algérie.

https://bit.ly/4hfzMVL



Rejoignez-nous au Sommet ICT Africa 2025, l'événement incontournable pour découvrir la prochaine vague des Technologies de l'Information et de la Communication (TIC) en Afrique. Ce rendez-vous majeur se tiendra du 21 au 23 avril 2025 au Palais des Expositions, Pavillon A, SAFEX, Alger, Algérie.

Le Sommet ICT Africa est la principale conférence et exposition dédiée à l'innovation numérique et aux avancées technologiques sur le continent africain. Cette année, sous le thème "Libérer les Horizons Numériques", l'accent sera mis sur le rôle transformateur des TIC pour stimuler la croissance économique et le développement durable en Afrique. Participez à des débats enrichissants sur des thèmes essentiels tels que l'inclusion numérique, la cybersécurité, l'intelligence artificielle et l'avenir du travail.

Référence	ANPT-2025-BV-03
Titre	Bulletin de veille N°03
Date de version	31 Mars 2025
Contact	ssi@anpt.dz