"The cost of cyber ignorance is far greater than the cost of cyber protection."

BULLETIN DE VEILLE N°01

ANPT-2025-BV-01

Janvier 2025

Alertes de sécurité

Fortinet

Fortinet corrige le zero-day de FortiOS exploité par des attaquants depuis des mois (CVE-2024-55591)

14 Janvier 2025

Fortinet a corrigé une vulnérabilité de contournement d'authentification (CVE-2024-55591) affectant ses pare-feux FortiOS et ses passerelles web FortiProxy, qui a été exploitée en tant que zero-day par des attaquants pour compromettre des pare-feux FortiGate exposés publiquement.

Bien que Fortinet ait reconnu l'exploitation dans l'avis de sécurité qui l'accompagne, la société n'a partagé aucune information relative à l'attaque, à l'exception des indicateurs de compromission (IoC) : adresses IP, entrées de journal, utilisateurs créés et liste des opérations effectuées par l'acteur de la menace.

Certains de ces IoCs recoupent ceux partagés par les chercheurs d'Arctic Wolf vendredi dernier, lorsqu'ils ont détaillé une campagne d'attaque qui a commencé à la mi-novembre et « a impliqué des connexions administratives non autorisées sur les interfaces de gestion des pares-feux, la création de nouveaux comptes, l'authentification VPN SSL par le biais de ces comptes, et diverses autres modifications de la configuration ».

CVE-2024-55591 est une vulnérabilité de contournement d'authentification (via un chemin ou un canal alternatif) qui permet à des attaquants distants d'obtenir des privilèges de super-administrateur via des requêtes élaborées vers le module websocket Node.js, leur permettant ainsi d'exécuter du code ou des commandes non autorisés.

Cette vulnérabilité critique affecte les versions 7.0.0 à 7.0.16 de FortiOS, ainsi que les versions 7.0.0 à 7.0.19 et 7.2.0 à 7.2.12 de FortiProxy. Elle peut être exploitée sans aucune interaction de l'utilisateur. Il a été conseillé aux administrateurs d'entreprise de mettre à jour vers une version corrigée - FortiOS 7.0.17 ou supérieur, FortiProxy 7.2.13 ou supérieur ou 7.0.20 ou supérieur - et de vérifier les indicateurs connus de compromission. Des solutions de contournement sont disponibles si la mise à jour de l'appliance n'est pas possible dans l'immédiat

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

Cisco

Cisco corrige une faille critique d'escalade de privilèges dans la gestion des réunions (CVSS 9.9)

24 Janvier 2025

Sophos Cisco a publié des mises à jour logicielles pour corriger une faille de sécurité critique affectant Meeting Management qui pourrait permettre à un attaquant authentifié à distance d'obtenir des privilèges d'administrateur sur les instances sensibles.

La vulnérabilité, répertoriée sous le nom de CVE-2025-20156, a un score CVSS de 9,9 sur 10,0. Elle a été décrite comme une faille d'escalade de privilèges dans l'API REST de Cisco Meeting Management.

« Cette vulnérabilité existe parce que l'autorisation appropriée n'est pas appliquée aux utilisateurs de l'API REST », a déclaré la société dans un avis publié mercredi. « Un attaquant pourrait exploiter cette vulnérabilité en envoyant des requêtes API à un point de terminaison spécifique.

« Une exploitation réussie pourrait permettre à l'attaquant d'obtenir un contrôle de niveau administrateur sur les nœuds de périphérie qui sont gérés par Cisco Meeting Management.

La vulnérabilité affecte les versions suivantes du produit, indépendamment de la configuration de l'appareil -

- Version 3.9 de Cisco Meeting Management (corrigée dans la version 3.9.1)
- Version 3.8 et antérieures de Cisco Meeting Management (migration vers une version corrigée)
- Version 3.10 de Cisco Meeting Management (non vulnérable)

Cisco a également corrigé 2 autres vulnérabilités, la première est CVE-2025-20165 (CVSS score : 7.5), une faille de déni de service (DoS) affectant BroadWorks, l'attaquant pourrait exploiter cette vulnérabilité en envoyant un grand nombre de requêtes SIP à un système affecté. Et la dernière vulnérabilité corrigée est CVE-2025-20128 (CVSS score : 5.3), une faille de type integer underflow impactant la routine de décryptage Object Linking and Embedding qui pourrait également résulter en une condition DoS.

Source : https://bit.ly/3PVgTva*F*

Actualité

Les pirates utilisent FastHTTP dans de nouvelles attaques à grande vitesse contre les mots de passe Microsoft 365

Des acteurs de la menace utilisent la bibliothèque FastHTTP Go pour lancer des attaques de mot de passe par force brute à grande vitesse ciblant les comptes Microsoft 365 dans le monde entier.

La campagne a été récemment découverte par la société de réponse aux incidents SpearTip, qui a déclaré que les attaques ont commencé le 6 janvier 2025, en ciblant l'Azure Active Directory Graph API.

Les chercheurs avertissent que les attaques par force brute ont réussi à prendre le contrôle de comptes dans 10 % des cas.

FastHTTP est un serveur HTTP haute performance et une bibliothèque client pour le langage de programmation Go, optimisé pour traiter les requêtes HTTP avec un débit amélioré, une faible latence et une grande efficacité, même lorsqu'il est utilisé avec de nombreuses connexions simultanées.

Dans cette campagne, elle est utilisée pour créer des requêtes HTTP afin d'automatiser les tentatives de connexion non autorisées.

SpearTip indique que toutes les requêtes ciblent les points d'extrémité Azure Active Directory pour forcer les mots de passe ou envoyer de manière répétée des défis d'authentification multi-facteurs (MFA) pour submerger les cibles dans les attaques MFA Fatigue.

SpearTip indique que 65 % du trafic malveillant provient du Brésil, en utilisant un large éventail de fournisseurs ASN et d'adresses IP, suivi de la Turquie, de l'Argentine, de l'Ouzbékistan, du Pakistan et de l'Irak.

Les chercheurs indiquent que 41,5 % des attaques échouent, 21 % conduisent à un verrouillage des comptes imposé par des mécanismes de protection, 17,7 % sont rejetées en raison de violations de la politique d'accès (conformité géographique ou de l'appareil) et 10 % étaient protégées par l'AMF.

Dans 9,7 % des cas, les auteurs de la menace parviennent à s'authentifier sur le compte cible, ce qui représente un taux de réussite particulièrement élevé.

Les prises de contrôle de comptes Microsoft 365 peuvent conduire à l'exposition de données confidentielles, au vol de propriété intellectuelle, à l'indisponibilité des services et à d'autres conséquences négatives.

SpearTip a partagé un script PowerShell que les administrateurs peuvent utiliser pour vérifier la présence de l'agent utilisateur FastHTTP dans les journaux d'audit, indiquant qu'ils ont été ciblés par cette opération.

Si des signes d'activité malveillante sont découverts, il est conseillé aux administrateurs d'expirer les sessions utilisateur et de réinitialiser immédiatement tous les identifiants de compte, d'examiner les dispositifs MFA enrôlés et de supprimer les ajouts non autorisés.

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

Un fournisseur d'accès russe confirme que des pirates ukrainiens ont « détruit » son réseau

Des hacktivistes ukrainiens, membres du groupe Ukrainian Cyber Alliance, ont annoncé mardi qu'ils avaient pénétré dans le réseau du fournisseur d'accès à Internet russe Nodex et effacé les systèmes piratés après avoir volé des documents sensibles.

« Le fournisseur russe d'accès à Internet Nodex à Saint-Pétersbourg a été complètement pillé et effacé. Les données ont été exfiltrées, tandis que l'équipement vide sans sauvegardes leur a été laissé », ont annoncé les hacktivistes ukrainiens sur Telegram.

Les pirates ont également partagé des captures d'écran des infrastructures virtuelles VMware, Veeam backup et Hewlett Packard Enterprise du FAI russe qu'ils ont piratées au cours de l'intrusion.

Mardi, Nodex a confirmé les affirmations de l'Ukrainian Cyber Alliance en annonçant à ses clients, dans un message sur VKontakte, que son « réseau était détruit » à la suite de ce qu'il a décrit comme une attaque planifiée provenant probablement d'Ukraine.

L'Ukrainian Cyber Alliance est active depuis 2016, lorsque plusieurs hackers et groupes de hackers (par exemple FalconsFlame, Trinity, RUH8 et CyberHunta) se sont regroupés pour défendre leur pays contre l'agression russe dans le cyberespace et se sont enregistrés en tant qu'organisation non gouvernementale.

Depuis lors, les cyberactivistes de l'UCA ont revendiqué de nombreuses violations touchant diverses organisations russes, notamment le ministère russe de la défense, l'Institut de la Communauté des États indépendants (financé par la société d'État russe Gazprom), le ministère du charbon et de l'énergie de la République populaire de Donetsk, le conseiller politique de Vladimir Poutine, Vladislav Surkov, ainsi que de nombreux officiers de l'armée et organes de presse russes, entre autres.

En octobre 2023, les hacktivistes ukrainiens ont également piraté les serveurs du gang du ransomware Trigona et les ont nettoyés après avoir exfiltré toutes les données, y compris le code source, les enregistrements de la base de données et les portefeuilles de crypto-monnaie.

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

Bon à savoir

Sensibilisation à l'ingénierie sociale : Se protéger contre les tactiques de manipulation

L'ingénierie sociale est une technique de manipulation psychologique utilisée par les attaquants pour exploiter le comportement humain et accéder à des informations ou des systèmes confidentiels. Contrairement au piratage technique, l'ingénierie sociale consiste à tromper les individus pour les amener à enfreindre les protocoles de sécurité. Les tactiques les plus courantes sont le phishing (hameçonnage), le pretexting (fabrication d'un faux scénario pour obtenir des informations), le baiting (offrir quelque

chose d'alléchant pour attirer une victime) et le tailgating (obtenir l'accès physique à des zones sécurisées en suivant le personnel autorisé). Ces méthodes exploitent la confiance, l'urgence, la curiosité ou la peur, faisant des individus le maillon le plus faible de la chaîne de sécurité. Une seule attaque réussie peut avoir de graves conséquences, telles que des pertes financières, des violations de données ou des atteintes à la réputation.

La sensibilisation et la vigilance sont les moyens de défense les plus efficaces contre l'ingénierie sociale. Les employés doivent être formés à reconnaître les demandes suspectes, à vérifier les identités avant de partager des informations sensibles et à remettre en question les communications inattendues, en particulier lorsque l'urgence est soulignée. Les organisations devraient mettre en place une authentification multifactorielle, mener des programmes réguliers de sensibilisation à la sécurité et encourager une culture du scepticisme dans le traitement des demandes non sollicitées. En outre, le signalement rapide des menaces potentielles peut contribuer à atténuer les risques et à prévenir d'autres attaques. En restant informés et proactifs, les individus et les organisations peuvent renforcer leurs défenses et réduire la probabilité d'être victimes de tactiques d'ingénierie sociale.

Evènements

Evènement à venir

International Conference on Cybersecurity Studies

17 feb 2025

Alger, Algérie

https://bit.ly/4hfzMVL

La conférence internationale sur les études de cybersécurité - Algérie 2025 servira de plateforme importante pour discuter des dernières avancées, des défis et des solutions dans le domaine de la cybersécurité. Cet événement prestigieux réunira des chercheurs, des professionnels de l'industrie et des experts qui participeront à des discussions approfondies, échangeront des connaissances et exploreront des stratégies innovantes pour renforcer la sécurité numérique. Il sera l'occasion d'aborder les cybermenaces émergentes, de partager des recherches de pointe et de favoriser la collaboration entre les principales parties prenantes dans le domaine de la cybersécurité.

Référence	ANPT-2025-BV-01
Titre	Bulletin de veille N°01
Date de version	31 Janvier 2025
Contact	ssi@anpt.dz