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

BULLETIN DE VEILLE N°04

ANPT-2025-BV-04

Avril 2025

Alertes de sécurité

Fortinet

Fortinet : Alerte sur des Vulnérabilités Critiques Touchant FortiGate et FortiSwitch

08 Avril 2025

Fortinet a récemment émis des alertes de sécurité concernant des failles critiques affectant ses produits FortiGate et FortiSwitch. Pour FortiGate, des cybercriminels exploitent trois vulnérabilités connues — CVE-2024-21762, CVE-2023-27997 et CVE-2022-42475 — pour insérer un fichier malveillant dans les systèmes compromis. Ce fichier permet un accès en lecture seule au système de fichiers, exposant potentiellement des données sensibles comme des configurations réseau.

Fortinet a pu identifier les clients concernés via sa télémétrie interne et leur a transmis des recommandations de remédiation. L'agence américaine CISA recommande la mise à jour immédiate vers les versions sécurisées de FortiOS (7.6.2, 7.4.7, 7.2.11, 7.0.17, 6.4.16). En parallèle, elle conseille de désactiver temporairement la fonction SSL-VPN, de réinitialiser les identifiants exposés, et de vérifier l'intégrité des configurations.

Par ailleurs, une autre vulnérabilité critique a été identifiée dans FortiSwitch, sous le code CVE-2024-4887, avec un score CVSS de 9.3. Elle affecte l'interface graphique (GUI) et peut permettre à un attaquant d'accéder à distance au système sans authentification, et de modifier les mots de passe administrateur. Cette faille a été découverte par un développeur interne, et aucun cas d'exploitation active n'a encore été signalé.

Les modèles vulnérables incluent FortiSwitch 7.6.0, 7.4.0 à 7.4.4, 7.2.0 à 7.2.8, 7.0.0 à 7.0.10 et 6.4.0 à 6.4.14. Des correctifs sont disponibles dans les versions suivantes : 7.6.1, 7.4.5, 7.2.9, 7.0.11 et 6.4.15. En attendant la mise à jour, il est recommandé de désactiver l'accès HTTP/HTTPS aux interfaces d'administration et de restreindre les connexions via des hôtes de confiance.

Cette faille fait partie d'un lot de dix vulnérabilités corrigées lors du Patch Tuesday d'avril 2025, dont certaines affectent d'autres produits Fortinet comme FortiAnalyzer, FortiManager ou FortiWeb. Certaines d'entre elles permettent des attaques de type man-in-the-middle. Fortinet rappelle l'importance de maintenir tous les équipements à jour, de surveiller activement les systèmes et de suivre les alertes de sécurité officielles.

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

Windows

Vulnérabilité Critique dans le Système de Mise à Jour de Windows (CVE-2024-43491)

22 Avril 2025

Une faille critique (CVE-2024-43491) a été découverte dans la pile de mise à jour (Servicing Stack) de Windows 10 version 1507, incluant les éditions Enterprise 2015 LTSB et IoT Enterprise. Cette vulnérabilité permet à un attaquant d'effectuer une attaque dite de "rollback", c'est-à-dire de restaurer une version antérieure du système, supprimant ainsi des correctifs de sécurité précédemment appliqués. Le score de gravité CVSS est de 9.8 sur 10, ce qui en fait une menace extrêmement sérieuse. Elle est déjà activement exploitée dans la nature, selon les chercheurs en sécurité.

La faille permet de contourner les protections d'intégrité du système et d'exécuter du code dans un environnement affaibli. Elle peut être utilisée pour réintroduire d'anciennes vulnérabilités déjà corrigées par Microsoft, rendant les systèmes vulnérables sans alerte visible. Microsoft a publié deux mises à jour à appliquer dans un ordre strict : d'abord KB5043936 (mise à jour du Servicing Stack), suivie de KB5043083 (mise à jour de sécurité). Ne pas suivre cet ordre peut rendre le correctif inefficace.

Les responsables IT doit impérativement vérifier leurs versions Windows et installer ces mises à jour sans délai. Il est aussi recommandé de renforcer la surveillance des fichiers système et des processus de mise à jour.

Cette faille rappelle l'importance d'un cycle de patching rigoureux, automatisé et contrôlé. Les organisations doivent s'assurer que les mises à jour critiques sont appliquées correctement, surtout dans les environnements sensibles.

Enfin, Microsoft encourage à surveiller les journaux système pour détecter d'éventuelles tentatives d'exploitation.

Source : https://bit.ly/4k0P8hH

Actualité

Blue Shield of California : Fuite de Données de Santé de 4,7 Millions de Membres vers Google

Blue Shield of California a récemment révélé une fuite de données affectant environ 4,7 millions de ses membres. Cette fuite résulte d'une mauvaise configuration de l'outil Google Analytics, utilisée entre avril 2021 et janvier 2024, qui a conduit au partage involontaire d'informations sensibles avec Google Ads.

Les données concernées incluent la taille de la famille, le sexe, le code postal, le type de plan d'assurance, les réclamations médicales et les recherches de prestataires de soins de santé. Bien que Google ait une politique interdisant la collecte de données de santé privées, ces informations ont pu être utilisées pour des campagnes publicitaires ciblées.

Blue Shield a découvert cette fuite en février 2024 et a immédiatement coupé la connexion entre Google Analytics et Google Ads. L'entreprise a également entrepris une révision de la sécurité de son site web et continue d'utiliser des outils d'analyse sous des protocoles révisés.

En parallèle, Blue Shield a été informée en septembre 2023 d'une autre violation de données impliquant un fournisseur tiers utilisant la plateforme MOVEit. Cette faille a exposé des informations telles que les noms, dates de naissance, numéros de sécurité sociale et données de traitement de la vue de certains membres.

En réponse, Blue Shield offre aux membres concernés une surveillance de crédit gratuite et des services de restauration d'identité. L'entreprise a également mis en place un centre d'appels dédié pour répondre aux questions des membres.

Plusieurs recours collectifs ont été déposés suite à ces incidents. Les autorités réglementaires, telles que le Département de la Santé et des Services sociaux des États-Unis, n'ont pas encore annoncé de mesures spécifiques contre Blue Shield ou Google.

Ces événements soulignent l'importance cruciale de la sécurité des données dans le secteur de la santé. Les organisations doivent s'assurer que leurs outils d'analyse et de transfert de données sont correctement configurés et conformes aux réglementations en vigueur pour protéger les informations sensibles des patients.

Source : ***https://bit.ly/3RQ3S78***

Japon : Alerte Nationale sur des Comptes Bancaires Piratés et des Transactions Frauduleuses

Le gouvernement japonais a lancé une alerte nationale après avoir détecté une série de transactions non autorisées effectuées via des comptes bancaires compromis. Ces incidents, survenus dans plusieurs institutions financières, concernent des transferts de fonds illicites réalisés à l'insu des titulaires de comptes. Les premières investigations suggèrent que les cybercriminels ont obtenu les identifiants des victimes via du phishing, des fuites de données tierces ou des infections par logiciels malveillants. Certaines connexions non sécurisées pourraient aussi avoir été exploitées. Face à ces attaques, les autorités japonaises collaborent avec les banques pour renforcer la sécurité des systèmes, notamment à travers la mise en place de l'authentification multifacteur et la surveillance accrue des activités inhabituelles. Plusieurs établissements ont temporairement suspendu certaines fonctionnalités de leurs plateformes en ligne afin de prévenir de nouvelles intrusions, tandis que les clients sont appelés à changer leurs mots de passe et à signaler tout mouvement suspect sur leurs comptes.

Dans le même temps, les enquêtes menées par les services gouvernementaux visent à déterminer l'origine exacte de ces compromissions. Le ministère de l'Économie, du Commerce et de l'Industrie et l'Agence des services financiers suivent l'évolution des cas avec attention, en coordination avec des fournisseurs de services cloud et des opérateurs télécoms pour tracer les connexions frauduleuses. Bien que le nombre exact de victimes reste inconnu, l'ampleur des activités suggère une campagne organisée à grande échelle, potentiellement pilotée depuis l'étranger. Cet événement met en lumière l'augmentation constante des attaques ciblant les services financiers au Japon depuis 2023. Dans ce contexte, le pays envisage de durcir ses obligations réglementaires en matière de notification des incidents de sécurité. Les autorités insistent sur la nécessité, pour les entreprises et les citoyens, de maintenir une hygiène numérique stricte. Cette crise souligne l'urgence d'améliorer la résilience collective face à des menaces cyber de plus en plus sophistiquées.

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

Bon à savoir

Phishing et Ingénierie Sociale : Les Armes Silencieuses des Hackers

Le phishing, aussi appelé hameçonnage, est une technique utilisée par les cybercriminels pour tromper les gens et voler des informations personnelles ou professionnelles. Cette méthode consiste à envoyer des messages frauduleux, souvent par e-mail, mais aussi par SMS ou via les réseaux sociaux. Ces messages imitent parfaitement ceux d'organisations connues, comme des banques, des services publics, des sites de commerce en ligne ou même votre propre entreprise. L'objectif est de vous faire croire qu'il y a une urgence : par exemple, que votre compte est bloqué, que vous devez confirmer une commande ou que vous avez gagné un cadeau. Ces messages contiennent des liens vers des sites web qui ressemblent aux vrais mais qui sont en réalité des copies créées pour voler vos données. En y entrant votre mot de passe, vos coordonnées bancaires ou d'autres informations, vous les envoyez directement à l'attaquant. Le phishing peut aussi vous pousser à télécharger un fichier infecté qui installe un virus sur votre appareil. Ce type de cyberattaque fonctionne parce qu'il joue sur la surprise, la peur ou la curiosité. Il est donc essentiel d'être prudent face aux messages inhabituels ou suspects, même s'ils semblent professionnels et bien rédigés.

L'ingénierie sociale, quant à elle, va encore plus loin. Elle repose sur la manipulation psychologique pour inciter une personne à agir contre ses propres intérêts, sans forcément utiliser la technologie. Le pirate peut, par exemple, se faire passer pour un collègue, un responsable ou un technicien, et vous appeler ou vous écrire pour vous demander un mot de passe, un accès ou une information confidentielle. Il peut créer un sentiment d'urgence ("c'est très important, c'est pour tout de suite") ou de confiance ("je travaille avec votre patron"). L'attaquant utilise des émotions comme la peur, la panique, l'urgence ou la politesse pour que vous ne preniez pas le temps de vérifier. Parfois, l'attaque peut même être physique : un faux livreur ou un faux technicien peut tenter de pénétrer dans un bureau pour accéder à un ordinateur. Ce type de menace est difficile à repérer car il ne s'agit pas d'un virus mais d'une personne qui sait comment manipuler les autres. Pour se protéger, il faut apprendre à reconnaître ces tentatives, toujours vérifier l'identité de la personne qui fait une demande inhabituelle, et ne jamais partager ses accès ou ses données sensibles à la légère. La formation, la méfiance, et l'habitude de signaler les comportements suspects sont des moyens efficaces pour se défendre contre ces attaques.

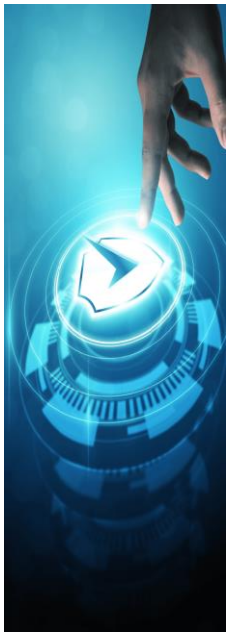
Evènements

Evènement à venir

Les huit plus grandes menaces pour votre entreprise et présentation des trois piliers de la cybersécurité 2025

08 Mai 2025 - Online

https://bit.ly/42WIfqS



L'événement intitulé « Les huit plus grandes menaces pour votre entreprise et présentation des trois piliers de la cybersécurité 2025 » est un atelier virtuel dédié aux enjeux majeurs de la cybersécurité auxquels sont confrontées les entreprises aujourd'hui.

Cet atelier mettra en lumière les huit menaces cybernétiques majeures auxquelles les entreprises doivent se préparer, tout en présentant les trois piliers fondamentaux de la cybersécurité à adopter en 2025. Les participants bénéficieront de conseils pratiques pour renforcer la sécurité de leur organisation face à un environnement numérique en constante évolution.

Référence	ANPT-2025-BV-04
Titre	Bulletin de veille N°04
Date de version	30 Avril 2025
Contact	ssi@anpt.dz