"Effective cybersecurity is not a product, but a process." – *Jim Langevin*

BULLETIN DE VEILLE N°07

ANPT-2025-BV-07

Juillet 2025

Alertes de sécurité

Outlook

Les serveurs Microsoft SharePoint attaqués par une vulnérabilité zero-day (CVE-2025-53770)

20 juillet 2025

Une nouvelle vulnérabilité critique, identifiée comme CVE-2025-53770, cible actuellement les serveurs Microsoft SharePoint sur site. Il s'agit d'une faille zero-day activement exploitée par des attaquants, sans correctif officiel au moment de la découverte. Cette faille permet à des acteurs malveillants non authentifiés de contourner l'authentification, d'installer des web shells et d'exécuter du code arbitraire à distance. Elle a été révélée comme une variante d'une vulnérabilité antérieure (CVE-2025-49706), supposée corrigée en juin, mais dont les correctifs se sont révélés insuffisants. L'exploitation de cette faille permet aussi d'extraire des clés cryptographiques sensibles (MachineKey), compromettant ainsi la sécurité globale du système.

Les attaques ont débuté vers le 18 juillet 2025, quelques jours après la publication des premiers correctifs incomplets. Microsoft a rapidement été alerté et a publié une alerte de sécurité, indiquant qu'aucune mise à jour n'était encore disponible à ce moment-là. Plusieurs groupes de cyberespionnage liés à la Chine, dont Linen Typhoon et Violet Typhoon, ont été identifiés comme étant responsables des attaques. Ces groupes ont ciblé des agences gouvernementales, des institutions énergétiques et de nombreuses organisations privées à travers le monde, y compris des entités critiques comme le National Nuclear Security Administration des États-Unis. Plus de 400 organisations auraient été touchées à ce jour.

Face à la gravité de la situation, Microsoft a finalement publié des correctifs d'urgence fin juillet pour SharePoint Server 2016, 2019 et Subscription Edition. L'éditeur recommande fortement aux administrateurs de serveurs d'appliquer les mises à jour immédiatement, de changer les clés MachineKey, d'activer AMSI pour renforcer l'analyse des scripts malveillants, et d'utiliser Microsoft Defender Antivirus pour détecter les web shells courants comme *spinstall0.aspx*. Les serveurs exposés à Internet avant la correction doivent être considérés comme compromis et faire l'objet d'un audit complet. Cette faille rappelle une fois de plus l'importance de corriger rapidement et de surveiller activement les environnements critiques.

Source : http://bit.ly/3HswaD0

VMWare

VMware fixes four ESXi zero-day bugs exploited at Pwn2Own Berlin

17 Juillet 2025

Lors du concours Pwn2Own Berlin 2025, quatre failles critiques ont été découvertes et exploitées avec succès sur les produits VMware, notamment ESXi, Workstation, et Fusion. L'exploit principal, CVE-2025-41236, est un integer overflow dans l'adaptateur VMXNET3 qui permet l'exécution de code sur l'hôte depuis une machine virtuelle invitée. Trois autres vulnérabilités, CVE-2025-41237 (integer underflow), CVE-2025-41238 (heap overflow), et CVE-2025-41239 (fuite d'informations via vSockets), ont également été démontrées par différentes équipes de chercheurs.

Suite à ces révélations, VMware (désormais propriété de Broadcom) a publié le bulletin de sécurité VMSA-2025-0013 le 15 juillet 2025. Des mises à jour correctives sont disponibles pour ESXi 7.x/8.x, VMware Workstation Pro 17.x, Fusion 13.x et VMware Tools. Les vulnérabilités critiques ont reçu un score CVSS de 9.3, soulignant leur capacité à provoquer une évasion de VM et une prise de contrôle complète de l'hôte. À ce jour, aucun cas d'exploitation active dans la nature n'a été détecté.

VMware recommande fortement aux utilisateurs de mettre à jour immédiatement leurs systèmes. Il n'existe aucune solution de contournement, ce qui rend l'application des correctifs essentielle. Les administrateurs sont également invités à revoir les privilèges accordés aux machines virtuelles et à renforcer la sécurité réseau interne. Cet incident met en évidence l'importance de la veille en cybersécurité, des tests en environnement isolé et de la réactivité face aux vulnérabilités zero-day.

Source : http://bit.ly/3UZTVp3

Actualité

France : une nouvelle violation de données pourrait affecter 340 000 demandeurs d'emploi

Un nouvel incident de cybersécurité majeur touche l'agence nationale France Travail. Le 13 juillet 2025, des attaquants ont compromis un compte utilisateur sans rôle élevé au sein d'un organisme de formation basé en Isère, à l'aide d'un logiciel de type infostealer, leur permettant d'accéder à Kairos, la plateforme de gestion des parcours des demandeurs d'emploi. Cette intrusion a entraîné la fuite potentielle des données personnelles de 340 000 personnes, incluant noms, adresses postales, adresses email, numéros de téléphone, identifiants France Travail et statuts de demandeur d'emploi. Heureusement, les mots de passe ainsi que les informations bancaires ne sont pas concernés par cette violation

L'agence a immédiatement mis hors ligne le portail compromis et tous les services associés à ses partenaires afin d'endiguer l'accès non autorisé. Le CERT-FR / ANSSI a détecté l'attaque le 12 juillet 2025 et coordonné la réponse avec France Travail. La remise en service de l'ensemble des plateformes est prévue pour le 24 juillet. Parallèlement, la CNIL a été notifiée et les autorités compétentes saisies. Les users concernés ont été alertés conformément aux obligations du RGPD, et la vaccination du système en matière de sécurité a été accélérée, notamment le déploiement de l'authentification à deux facteurs (2FA) pour Kairos, initialement prévu pour 2026

Cet incident intervient moins de deux ans après une fuite encore plus massive ayant exposé jusqu'à 43 millions de comptes entre février et mars 2024, rendant ce second cas particulièrement préoccupant. Même si les données divulguées cette fois-ci ne comprennent pas d'informations financières, elles demeurent très sensibles et prédisposent les victimes à des attaques de phishing, tentatives d'usurpation d'identité ou d'arnaques liées à de fausses offres d'emploi. France Travail a mis en garde les utilisateurs à rester particulièrement vigilants face à toute sollicitation non sollicitée. Pour prévenir de nouvelles compromissions, il est recommandé d'installer des mesures de sécurité accrues, de segmenter les droits d'accès, et d'effectuer des audits réguliers des systèmes interconnectés avec des services tiers

Source : http://bit.ly/4fqBnYw

Une cyberattaque porte un coup dur au firmware russe utilisé pour réutiliser des drones civils pour la guerre en Ukraine

Un cyberincident ciblant l'infrastructure de distribution du firmware militaire russe "1001" a été confirmé par les développeurs russes concernés. Ce firmware, utilisé pour convertir des drones civils DJI en drones résistants au GPS spoofing pour l'effort de guerre en Ukraine, est distribué via des terminaux spécialisés. Les attaquants ont compromis les serveurs de mise à jour, affiché des messages falsifiés sur les terminaux des opérateurs et bloqué leur fonctionnement, empêchant la diffusion du firmware. Bien que le firmware lui-même ne soit pas compromis — les développeurs jugent le risque de backdoor "très faible" — les opérations de mise à jour ont été interrompues .

Cet incident, révélé début juillet 2025, touche potentiellement près de 200 000 drones déjà reprogrammés avec la version 1001 au moment de l'attaque. L'expert russe Oleg Shakirov, cité sur Telegram, a indiqué que l'intrusion visait très probablement le serveur distant chargé de délivrer les mises à jour aux terminaux des centres de service. À l'heure actuelle, aucun groupe n'a revendiqué l'opération, mais l'attaque démontre une connaissance précise de la cible, qui repose sur une infrastructure hautement spécialisée .

Même si aucune porte dérobée ou altération malveillante du firmware n'a été détectée, les conséquences sont militaires : sans accès aux terminaux, l'armée russe pourrait être incapable de reconfigurer ou mettre à niveau rapidement ses drones convertis. Les opérateurs ont été invités à déconnecter temporairement leurs terminaux pour limiter tout risque supplémentaire. Cet incident rare souligne la vulnérabilité des chaînes d'approvisionnement technologiques militaires, même pour des systèmes apparemment isolés de la guerre cybernétique traditionnelle

Source : http://bit.ly/3USJq73

Bon à savoir

Éviter les fausses « offres à durée limitée »

Sur internet, on voit souvent des messages du type "Offre exceptionnelle valable 24h !" ou "Seulement 5 articles restants ! Dépêchez-vous !". Ces messages sont faits pour créer un sentiment d'urgence et vous pousser à acheter sans réfléchir. Dans la plupart des cas, ces offres ne sont pas réelles. Elles sont conçues pour vous faire cliquer rapidement, sans vérifier si le site est fiable ou si l'article vaut vraiment le prix affiché. Il faut apprendre à rester calme et à ne pas se laisser piéger par cette pression artificielle.

Les escrocs utilisent souvent ces "offres limitées" pour vendre de faux produits, collecter vos données personnelles, ou même voler vos informations bancaires. Un site douteux peut ressembler à une vraie boutique en ligne, avec des logos connus et des fausses évaluations clients. Avant de faire un achat, prenez le temps de vérifier l'URL du site, cherchez des avis indépendants et posez-vous cette question : "Est-ce trop beau pour être vrai ?" Si un iPhone est affiché à moitié prix pendant 30 minutes seulement, c'est probablement une arnaque. La vraie rareté n'a pas besoin de vous harceler avec des compteurs et des alertes.

Pour éviter ces pièges, ne cliquez jamais sur les liens envoyés par SMS, email ou sur les réseaux sociaux sans vérifier leur origine. Utilisez des sites de confiance et privilégiez les plateformes connues. Méfiez-vous aussi des publicités qui promettent des cadeaux gratuits ou des réductions énormes "juste aujourd'hui". Activez les notifications de sécurité sur votre navigateur et installez une extension qui vous alerte en cas de site suspect. Enfin, souvenez-vous : une bonne affaire ne disparaît pas en 5 minutes. Mieux vaut rater une fausse promo que de perdre votre argent ou vos données.

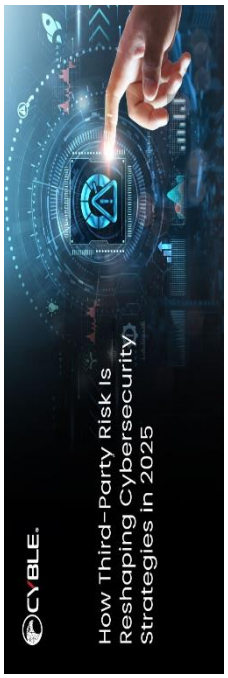
Evènements

Evènement à venir

Managing Third-Party Cyber Security Risk 2025

05-06 Août 2025 - Online

http://bit.ly/3UmCmiP



L'événement intitulé « Gérer les risques de cybersécurité liés aux tiers » vise à fournir aux participants une compréhension globale de l'importance de la gestion des cyberrisques liés aux fournisseurs tiers. Cette formation en ligne permettra d'identifier et d'évaluer les risques potentiels que ces fournisseurs représentent pour les opérations commerciales et la sécurité des données. Les participants découvriront le paysage actuel des cybermenaces liées aux tiers et acquerront les connaissances nécessaires pour mettre en œuvre des stratégies efficaces d'atténuation et de gestion de ces risques. La formation abordera les contrôles essentiels et les bonnes pratiques indispensables au maintien de la cybersécurité dans le cadre des relations avec des tiers.

Référence	ANPT-2025-BV-07
Titre	Bulletin de veille N°07
Date de version	31 Juillet 2025
Contact	ssi@anpt.dz